RES Workspace Manager 2014
Self-Study Kit

Contents

Chapter 1: Introduction 1

Chapter 2: Video Tutorials 2

Chapter 3: User Workspace Management 5

3.1 Introduction to User Workspace Management 5

Chapter 4: Architecture 8

4.1 Components 8
4.1.1 The RES Workspace Manager Console 8
4.1.2 The RES Workspace Manager Datastore 9
4.1.3 The RES Workspace Manager Agents 9
4.1.4 RES Workspace Manager Relay Servers 11
4.1.5 The RES Workspace Composer 12
4.2 Communication Model 13
4.3 The RES Workspace Manager Agent Service and its sub processes 14
4.4 The RES Workspace Manager Agent Cache 15

Chapter 5: Installation & Setup 16

5.1 Prerequisites 17
5.2 Installing RES Workspace Manager and Configuring the Shell 19
5.3 Configuring the Shell - Centralized Computing 22
5.4 Setting up the Datastore 24
5.5 Configuration Wizard 26
5.6 Relay Servers 31
5.7 Agents 36
5.8 RES Workspace Manager Licensing 39
5.8.1 Licensing Model 39
5.8.2 Licensing Process 41
5.8.3 Managing Licenses 43
5.9 RES Workspace Manager modules 45
5.10 Directory Services 47
5.10.1 Novell Directory Services 49
5.11 Workspace Branding 51

Chapter 6: Access Control 52

6.1 Identity 52
6.2 Locations and Devices: Zones 56
6.2.1 Zone rules 56
6.2.2 Multiple Rules for a Zone 60
6.2.3 Zone Members: Nested Zones 61
6.2.4 Pattern matching in Zones 61
6.2.5 Example: Using a USB device for authentication purposes 62
6.3 Connection States 63
6.4 Languages 64
6.5 Application Delegation 65

6.6 Administrative Roles 67
6.6.1 Scope Control 69
6.7 Filters 71

Chapter 7: Composition 74

7.1 The End-User Workspace 74
7.1.1 The Workspace Composer 75
7.1.2 Workspace Preferences 77
7.1.3 Printing Preferences 80
7.1.4 PowerHelp 81
7.2 Desktop Transformation 82
7.2.1 Introduction to Desktop Transformation 82
7.2.2 Desktop Sampler 83
7.2.3 Workspace Designer 85
7.2.4 Workspace Model 86
7.2.5 Managed Applications 86
7.3 Application Management 87
7.3.1 Applications 87
7.3.2 Start Menu Tab 87
7.3.3 Settings tab 88
7.3.4 Configuring Applications 93
7.3.5 File Types 107
7.3.6 E-mail Settings 108
7.3.7 Data Sources 109
7.3.8 Workspace Extensions 110
7.4 Actions 112
7.4.1 Drive and Port Mappings 112
7.4.2 Drive Substitutes 115
7.4.3 Folder Redirection 116
7.4.4 Folder Synchronization 119
7.4.5 Directory Maintenance 121
7.4.6 Printers 123
7.4.7 User Registry 125
7.4.8 Execute Command 130
7.4.9 Microsoft System Center Configuration Manager Software Distributions 131
7.4.10 LANDesk 132
7.4.11 Automation Tasks 133
7.4.12 Environment Variables 135
7.4.13 Linked Actions 136
7.5 Desktop 137
7.5.1 Shell 137
7.5.2 Background 138
7.5.3 Lockdown and Behavior 139
7.5.4 Screensaver 139
7.6 User Settings 140
7.6.1 Zero Profile Modes 141
7.6.2 Migration settings when switching to another Zero Profile mode 150
7.6.3 What is saved as part of a Targeted Item 151
7.6.4 Storage of users' User Setting data 152
7.6.5 Additional User Setting options 155
7.6.6 Microsoft App-V applications 160
7.6.7 Citrix streamed applications 160

Chapter 8: Integration 161

8.1 Alerting 161
8.2 Application Virtualization 163
8.2.1 Citrix XenApp Publishing 163

8.2.2 Citrix XenApp Streaming 170
8.2.3 Microsoft App-V 171
8.2.4 Microsoft TS RemoteApp 173
8.2.5 Generic Isolation Integration 176
8.3 Microsoft Remote Assistance 180
8.4 Microsoft System Center 181
8.5 LANDesk 182
8.6 RES Software 183
8.6.1 RES Automation Manager 184
8.6.2 RES HyperDrive 186
8.6.3 RES IT Store 187
8.6.4 RES VDX 188
8.7 Web Portal 191

Chapter 9: Tracking and Reporting 192

9.1 Usage Tracking 192
9.2 Usage Tracking Overview 194
9.3 User Sessions 195
9.4 Workspace Simulation Wizard 197
9.5 License metering 201
9.6 Audit Trail 203

Chapter 10: Security & Performance 204

10.1 Security 204
10.1.1 Applications 205
10.1.2 Data 214
10.1.3 Authorized Files 218
10.1.4 User Sessions security 219
10.1.5 Network Connections security 220
10.2 Performance 225
10.2.1 Access Balancing 225
10.2.2 CPU Optimization 226
10.2.3 Instant LogOff 227
10.2.4 Memory Optimization 229

Chapter 11: Management 231

11.1 Building Blocks 231
11.2 Instant Reports 234
11.3 Workspace Containers 235
11.4 Workspace Analysis 241
11.5 Errors 244

Chapter 12: Contact Information 245

Chapter 13: Index 247

Chapter 1: Introduction

Welcome to the RES Workspace Manager 2014 Self-Study Kit. This document provides detailed information about the installation and configuration of RES Workspace Manager 2014 features and components.

Chapter 2: Video Tutorials

Various video tutorials are available that provide you with more information about RES Workspace Manager. These tutorials cover a broad range of subjects, from planning, installing and setting up an environment to using the functionality of RES Workspace Manager.

Video tutorials can be accessed from the RES Workspace Manager Help:

- A complete list of all available video tutorials by category can be found in the Help, by clicking **Help > Video Tutorials** from the menu bar of the Console.
- Depending on availability, individual tutorials can be accessed from the matching Help topic, by clicking **View tutorial**.

The following video tutorials are available for RES Workspace Manager:

An Introduction to Workspace Management

Infrastructure

Communication Model

Installation and setup

Installing RES Workspace Manager

Setting up the Datastore

Splitting the Datastore

Licensing

Configuring the Agents and Setting the Shell (Terminal Server)

Configuring the Agents and Setting the Shell (Workstation)

Setting up Directory Services

Locations and devices

Desktop Transformation

- Installing the Desktop Sampler and using the Workspace Designer
- Using the Workspace Model and Managed Applications

Composition

- The end user environment and utilities
- Creating Managed Applications
- Managed Applications: File Types
- Managed Applications: E-mail templates
- Managed Applications: Data Sources
- User Settings: Capture targeted items on session end using a template (global)
- User Settings: Capture targeted items, then track further changes
- User Settings: Track Any Setting Changed by Application Immediately
- User Settings: User Settings caching
- Printers
- Drive Substitutes
- Folder Synchronization
- Directory Maintenance
- Background & Screensaver
- Lockdown and Behavior
- User Registry
- Execute Command
- Environment Variables & Drive and Port Mapppings

Integration

RES Automation Manager Integration / Automation Tasks

MS App-V Integration

Workspace Containers - RES VDX Integration

Generic Isolation Integration

Web portal

Management

Building Blocks

Instant Reports

Workspace Containers

Workspace Analysis

Navigation Map

Application License Metering

Dynamic Privileges (Managed Applications)

Dynamic Privileges (User Installed Applications)

Process Interception

Chapter 3: User Workspace Management

User Workspace Management, with its dynamic composition and excellent security features, saves IT professionals' time and it allows users to stay productive while maintaining security wherever they are. This chapter describes what user workspace management is, what it does, and how it works.

3.1 Introduction to User Workspace Management

What is User Workspace Management?

The best way to explain User Workspace Management is to take a regular Microsoft Windows desktop as a starting point. There are important items on the desktop that enable productivity of the end user, such as e-mail applications, access to shared documents and the ability to print documents. There are also useful items on the desktop that make it more comfortable, such as personalized settings for using the e-mail application, a favorite background picture or other preferences. These useful items do not directly affect productivity, but do make life easier.

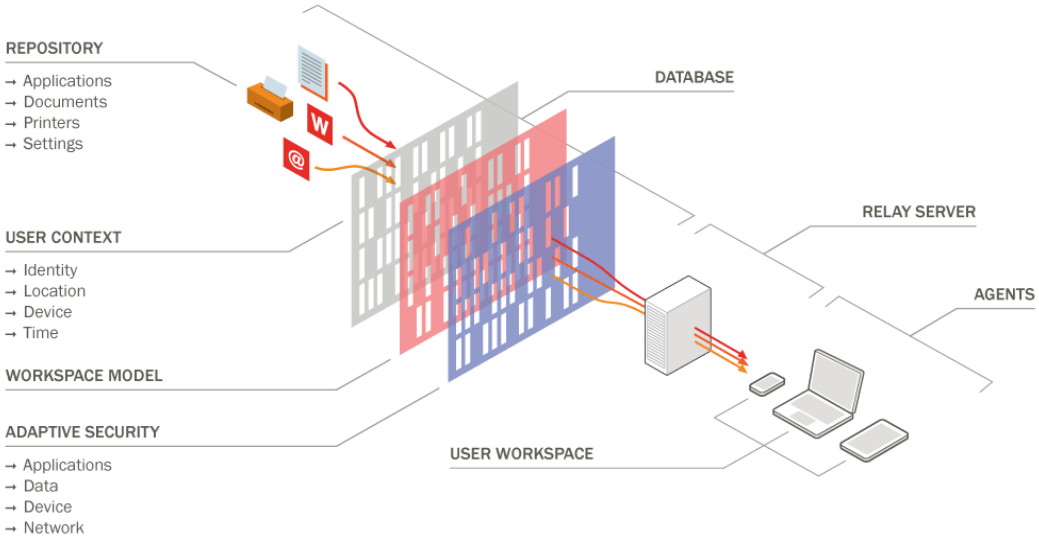
Desktop items include:

1. Applications
2. Documents and other data
3. Printing capabilities
4. Personal settings

The availability of desktop items depends on the computer and the user account that are used. Using a different computer or a different user account do not guarantee availability of the same list of desktop items.

A User Workspace is composed each time you log in to a Windows desktop. After composition, the desktop contains configured applications, data, printing capabilities and personal settings. Composition of these items is dynamic and based on context (who you are, where you are, what computer you use and the time of day).

Once the unique User Workspace has been composed, it is secured simply and effectively by only allowing the use of the available workspace items. The User Workspace exists until the user logs off from the Windows desktop.



Composing and Securing a User Workspace only takes seconds and is independent from any underlying technologies. User Workspace Management allows you to manage this process easily for many user workspaces at once.

How User Workspaces are composed

First, the administrator sets up how the context will be established during composition of the User Workspace. The administrator then creates a list of all possible desktop items that need to be managed in a User Workspace. For each item on this all-encompassing list, the administrator defines for whom, where, when and how the item should appear in a User Workspace.

This information is stored in a central database and is distributed to each Windows desktop. The Workspace Composer running on the Windows desktop will use this information to:

1. Establish the identity and location of the user
2. Determine the time of day and type of computer
3. Match every desktop item with the established context
4. Check the availability of allowed desktop items (workspace items)
5. Configure and show each workspace item
6. Detect any changes to the established context

The Workspace Composer starts when a new Windows session is started on a virtualized or physical desktop, online or offline laptop, or terminal server. The Workspace Composer evaluates each detected change to the established context (e.g. disconnecting from the network, reconnecting to a remote desktop session, launching an application) and recomposes specific parts of the User Workspace as necessary. In addition, it collects information about the session and sends it back to the central database.

How User Workspaces are secured

Once the unique User Workspace has been composed, the workspace items automatically indicate what is allowed in a User Workspace. The User Workspace is secured by disallowing anything else. The following items can be secured:

- Applications
- Removable Disks
- Files and Folders
- Network
- Sessions
- Locations and Computers

Security rules, stored in the same central database, are used by the Workspace Composer to set up security. The level of security can be controlled through these rules and can range from loose to very tight. The built-in security engines process the context aware information from the Workspace Composer. These engines are capable of blocking any unauthorized application, file or network access. Security diagnostics and logging are sent back to the central database.

Chapter 4: Architecture

4.1 Components

RES Workspace Manager consists of a central database (Datastore) and several software-based components. Each component relies on the Datastore for timely information regarding the user's environment.

4.1.1 The RES Workspace Manager Console

The RES Workspace Manager Console is the central point of administration of the User Workspace. It is usually run from an administrator's workstation. The Management Console stores all the provided information in a database.

In the Management Console, the administrator can centrally manage context-aware workspaces that contain all of the right applications, data, printing and personal settings essential for the users' productive working. It offers the Workspace Designer and several Wizards, helping the administrator to create workspace items according to business rules and compliance. With the Workspace Model the administrator can control which parts should be composed and secured in the User Workspace.

Throughout the Console the size of the columns as they appear on screen can be adjusted. Customized column width or order of columns is saved automatically on the user's home drive or, if not available, in the user's registry. The option **Reset all column properties to defaults** in the **Options** menu, will reset any changes that you made to the order or widths of columns in the Console.
In every list view in the Console, one colum is by default configured to autosize to fill out any remaining screen width. If you adjust the width if an autosizing column, it will no longer autosize and so you may end up with white space to the left of the columns.

The RES Workspace Manager Console process, `pwrtech.exe`, has only one instance per device.

Some of the Wizards run as a single instance subprocess called `wmwizrds.exe`.

4.1.2 The RES Workspace Manager Datastore

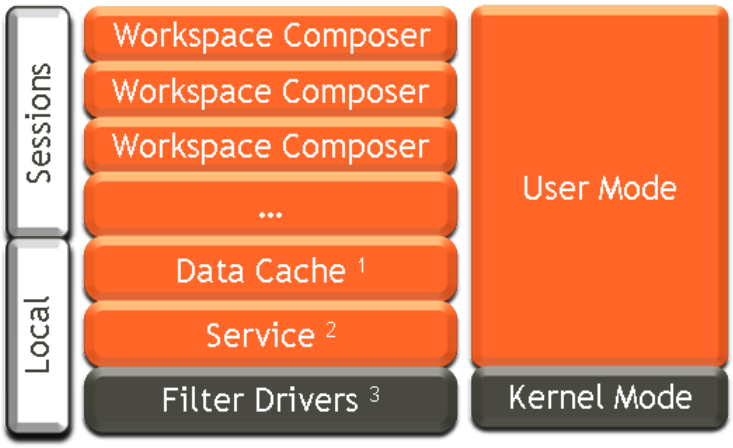
The Datastore is the central database for your RES Workspace Manager environment. All computers in a RES Workspace Manager environment connect to this database. It runs on a central Database server that you have installed prior to installing the RES Workspace Manager Console.

The Datastore can exist on any of the following Database types:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008 x86/x64
- Microsoft SQL Server 2008 R2 x86/x64
- Microsoft SQL Server 2012
- Microsoft SQL Azure
- IBM DB2 9.1 or higher x86/x64
- MySQL 5.0 or higher x86/x64
- Oracle 9i or higher x86/x64

4.1.3 The RES Workspace Manager Agents

An important aspect of RES Workspace Manager RES Workspace Manager 2014 is the architecture of each RES Workspace Manager Agent (i.e. each Terminal Server, workstation or laptop that runs RES Workspace Manager). The following illustration provides a schematic overview:



[1] Log files, Objects, Registry Settings
[2] RES Workspace Manager Agent Service
[3] NetGuard, AppGuard, RegGuard

Configuration data received from the Datastore is cached locally. Each RES Workspace Manager Agent uses its cached data instead of connecting to the SQL database directly.

The data cache also stores user information (log files and monitoring data) that is collected by each RES Workspace Manager Agent. The RES Workspace Manager Agent Service sends this data from the local cache to the Datastore for centralized access from the Management Console.

Read more about the RES Workspace Manager Agent Service (`res.exe`) and about the communication processes to and from the Datastore in the chapter "The RES Workspace Manager communication architecture".

Each Agent Cache consists of:

- log files
- objects
- registry settings

Log files

The log files contain monitoring files, error logs and PowerTrace data from RES Workspace Manager end-user components. These files are stored in a dedicated cache folder:

```
%programfiles%\RES Software\Workspace Manager\Data\DBCache\Transactions
```

They are forwarded to the RES Workspace Manager Datastore by the RES Workspace Manager Agent Service.

Objects

The objects stored in the local cache are XML files containing part of the RES Workspace Manager configuration data, and various resources in different formats.

These files are stored in subfolders of `%programfiles%\RES Software\Workspace Manager\Data\DBCache`:

- **\Objects** contains .xml files specifying application settings, PowerLaunch settings and other configuration settings.
- **\IconCache** contains icons for your programs and shortcuts.
- **\Resources** contains a number of subfolders that store your `.ica` files, `.osd` files, `.adm` files, files used as desktop images, and files used in your folder maintenance. The \Resources folder functions much like a distributed fileshare.

The RES Workspace Manager Agent Service forwards these objects from the RES Workspace Manager Datastore to the local cache.

Registry Settings

The remainder of the RES Workspace Manager configuration data is implemented as Registry settings. The data is forwarded from the RES Workspace Manager Datastore to the agent cache by the RES Workspace Manager Agent Service, and is stored in the following registry key:

```
HKLM\Software\Policies\RES\Workspace Manager\Settings
```

This concerns settings that have a restricted set of possible values, such as:

- MemoryShield > "Enabled": the value of the setting can only be "Yes" or "No".
- Maximum number of simultaneous logons: the value of the setting can only be a number.

You can define exceptions per user by customizing the registry key:

```
HKCU\Software\Policies\RES\Workspace Manager\Settings
```

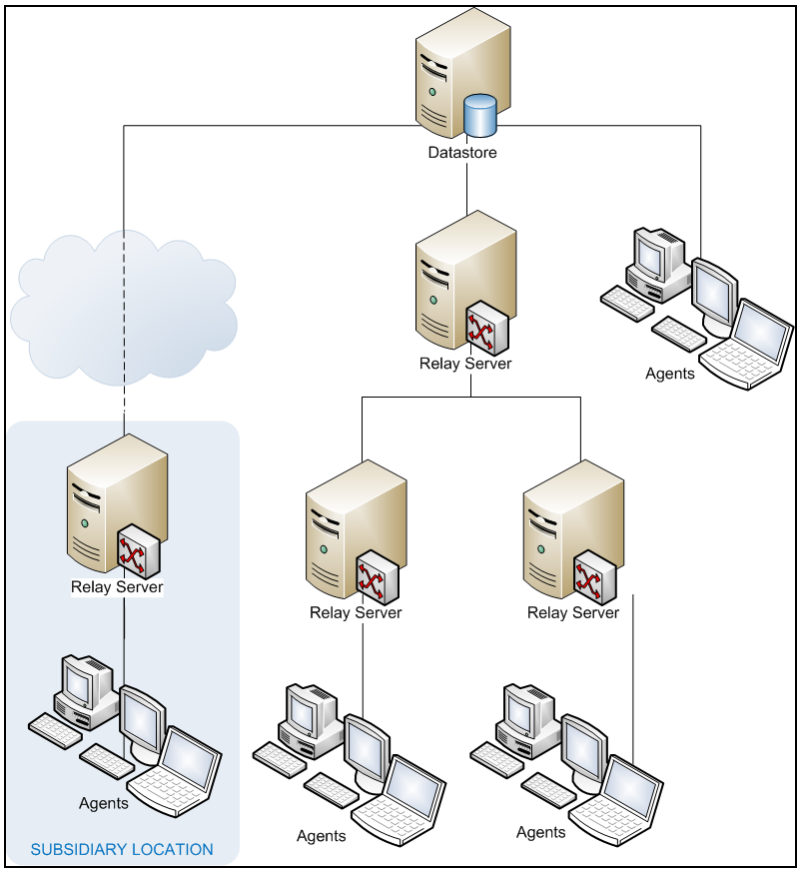
These exceptions can be implemented using the RES Workspace Manager **Actions** technology.

4.1.4 RES Workspace Manager Relay Servers

The Relay Server component makes it possible to create a flexible architecture that consolidates and centralizes all RES Workspace Manager configuration data into one central database, while ensuring that dispersed Agents across multiple sites obtain configuration data efficiently and in a timely manner.

Relay Servers are an optional infrastructure component. Relay Servers cache information from the Datastore and pass it on to Agents or to other Relay Servers. Agents can be configured to contact the Datastore directly, or to use Relay Servers.

In a RES Workspace Manager site, both methods can be used at the same time, with some Agents connecting the Datastore and others using Relay Servers.



Relay Servers offer a number of advantages:

- Improved scalability in all kinds of distributed network topologies.
- Reduced network traffic in multiple-site environments, as fewer components connect directly to the central Datastore over relatively slow data connections.
- Reduced datastore load, as fewer components connect directly to the central Datastore.
- Agents that connect to Relay Servers do not need to have a database driver installed for the RES Workspace Manager Datastore.

For further details about Relay Servers, see the document **Getting Started with RES Workspace Manager 2014 Relay Servers**, which is available at www.ressoftware.com/support.

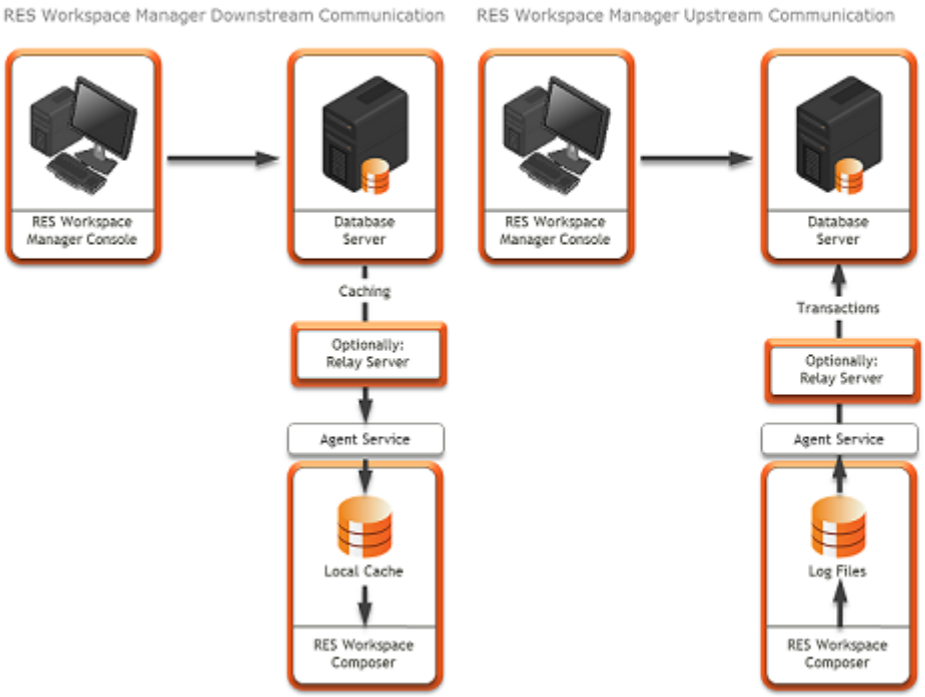
4.1.5 The RES Workspace Composer

The RES Workspace Composer is the RES Workspace Manager-managed uniform workspace that the end users are presented with, regardless of the technology stack used. The RES Workspace Composer provides only the functionality that the end user needs. This includes all applications, menu items and settings to which the user is granted access.

The desktop can be displayed using either the RES Workspace Manager shell or the Microsoft Windows shell. Both shells are managed by RES Workspace Manager, but the RES Workspace Manager shell presents a classic windows-like shell with some additional RES Workspace Manager-only technology, whereas the Microsoft Windows shell is the exact shell as it is presented by Microsoft, including the various available themes. After installation of RES Workspace Manager you need to configure the RES Workspace Composer as the default shell for your users.

4.2 Communication Model

RES Workspace Manager stores all configuration data and resources in an SQL-based database: the RES Workspace Manager Datastore. You can set all your Terminal Servers, Desktops and laptops to use a single database or you can use replication to set up multiple databases.



The RES Workspace Manager Console communicates directly with the RES Workspace Manager Datastore. All RES Workspace Manager Agents receive a local cache of the RES Workspace Manager Datastore and communicate with their cache rather than directly with the RES Workspace Manager Datastore.

The local cache stores configuration data that is received from the Datastore. Each RES Workspace Manager Agent uses its cached data instead of connecting to the SQL database directly.

The local cache also stores user information (log files and monitoring data) that is collected by each RES Workspace Manager Agent. The **RES Workspace Manager Agent Service**, which runs on each RES Workspace Manager Agent, sends this data from the local cache to the Datastore.

Local caches are updated through selective synchronization: the RES Workspace Manager Agent Service retrieves only changed information from the Datastore to place in the local data cache. This reduces the load on the central database significantly. This downstream communication is asynchronous: if the database is busy or unavailable, the request is deferred until the database is able to process it.

The RES Workspace Manager Datastore also stores the user information (log files and monitoring data) that is collected by all RES Workspace Manager Agents. The RES Workspace Manager Agent Service pushes each Agent's log files and monitoring information from the local cache to the Datastore. This upstream communication is also asynchronous: if the database is busy or unavailable, the information remains in cache until the database is able to receive it.

4.3 The RES Workspace Manager Agent Service and its sub processes

Each desktop that has the RES Workspace Composer installed has an agent service that retrieves the information from the database and stores it locally. The Workspace Composer running on the Windows desktop will use this local information and the context of the user to compose and secure (parts of) the User Workspace. As someone works in their User Workspace information is collected by the Workspace Composer in transactions. These transactions are applied to the central database by the agent service whenever it can access the central database

The RES Workspace Manager Agent service is named `Res.exe` (service as local system). `Res.exe` and its sub processes have only one instance per device.

- The following information is stored at `HKLM\Software\RES\Workspace Manager`:

  `Root` – Datastore Connection Properties

  `UpdateGUIDS` – UpdateGUIDs

  `Data` – Access Balancing

  The tasks of the RES Workspace Manager Agent Service (`Res.exe`) consist of:

  - Checking Datastore connectivity
  - Unlocking and locking the user Registry
  - Handle License requests (session and application)
  - Handle logging
  - Check its own running processes

  The RES Workspace Manager Agent Service contains the following sub processes:

- resop
- Pwrcache
- Pwrcache /upload
- CPUShield (CPU Optimization)
- isloggoff

  pwrcache.exe

  The tasks of the `pwrcache.exe` sub process are:

- Update the Agent Cache from the RES Workspace Manager Datastore
- Agent Cache Resources, XML and registry
- Updates are based on GUID tree information

  - Pwrcache.exe /upload
- Upload Agent/Session stored logging to the RES Workspace Manager Datastore from `%programfiles\RES Software\Workspace Manager\Data\DBCache\transactions`

4.4 The RES Workspace Manager Agent Cache

- There is one RES Workspace Manager Agent Cache per device.
- The RES Workspace Manager Agent Cache is located at: `%programfiles%\RES Software\Workspace Manager\Data\DBCache\`
- The sub folders contain the following data:

`IconCache` – contains icons for programs and shortcuts

`Objects` – contains `.xml` files specifying Application, and other configuration settings

`Resources` – contains a number of subfolders that store files like `osd`, `.ICA`, `.bmp` etc.

`Transactions` – Log files waiting for transfer

`HKLM\Software\Policies\RES\Workspace Manager\Settings\....` – Integer values and Booleans

- A User Session only needs **read** permissions on Agent Cache.
- The Agent Cache is protected by RES Workspace Manager Security.

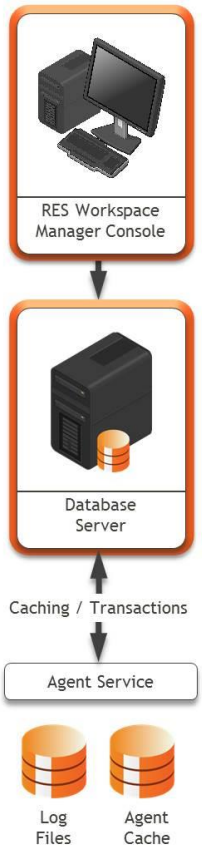
Chapter 5: Installation & Setup

RES Workspace Manager 2014

In this course we will first deal with a "clean" installation of RES Workspace Manager. All features will be dealt with from the perspective of setting up a new environment. When you are familiar with all features and technologies of RES Workspace Manager we will go into the subject of Desktop Transformation.

In this chapter we will take you through the process of installing RES Workspace Manager. In general, the RES Workspace Manager installation process is the same, regardless of the underlying technology stack.

Besides a full installation of RES Workspace Manager, you can also install only the Console. This would typically be done to administer an existing RES Workspace Manager environment. This type of installation does not install the RES Workspace Manager Agent Service, or the AppGuard and NetGuard drivers, and it will use an existing database.



5.1 Prerequisites

	Prerequisites
Software	One of the following RES Workspace Manager installation files, available for download at http://www.ressoftware.com/downloads: ▪ `RES-WM-Installer-2014.exe` - This is an installation package that contains the `.msi` files for the RES Workspace Manager components. Individual components can be extracted from the installer and are also available for download. If you want to use the Relay Server, separate installation files are required. The installation of Relay Server requires Microsoft .NET Framework 4.0 or higher. For more information, please refer to the document **Getting Started with Relay Servers**.
Software installed on Agent	▪ Microsoft .NET Framework 2.0 or higher. Microsoft .NET Framework 4 Client Profile or higher when using User Setting caching. ▪ One of the following operating systems: ▪ Microsoft Windows 2003 x86/x64 ▪ Microsoft Windows 2003 R2 x86/x64 ▪ Microsoft Windows XP x86/x64 ▪ Microsoft Windows Vista x86/x64 ▪ Microsoft Windows 2008 x86/x64 ▪ Microsoft Windows 2008 R2 x64 ▪ Microsoft Windows 2012 x64 ▪ Microsoft Windows 2012 R2 x64 ▪ Microsoft Windows 7 x86/x64 ▪ Microsoft Windows 8 x86/x64 ▪ Microsoft Windows 8.1 x86/x64
Hardware	▪ Each full installation of RES Workspace Manager requires approximately 104 MB of hard disk space for the application files. This does not include the data stored in the local cache. The hard disk space required for cached data entirely depends on the configuration of your RES Workspace Manager environment. Each Console-only installation of RES Workspace Manager requires approximately 48 MB of hard disk space. These installations do not require any additional disk space for the local cache. Each Agent-only installation of RES Workspace Manager requires approximately 64 MB of hard disk space. ▪ Each RES Workspace Manager Agent requires 22 MB of memory. Each user requires a small amount of network drive space on the home drive for storing RES Workspace Manager settings. This amount will increase if User Settings are available to the user, because User Settings are stored in the same location. The required amount of space then depends on the size of the stored User Settings.
Database	One of the following databases: ▪ Microsoft SQL Server 2005 ▪ Microsoft SQL Server 2008 x86/x64 ▪ Microsoft SQL Server 2008 R2 x86/x64 ▪ Microsoft SQL Server 2012 ▪ Microsoft SQL Azure ▪ IBM DB2 9.1 or higher x86/x64 ▪ MySQL 5.0 or higher x86/x64 ▪ Oracle 10.2 or higher x86/x64

Database prerequisites	
Microsoft SQL Server 2005 and later (including express editions)	▪ Mixed Mode authentication ▪ MDAC 2.6 or later on all Agents ▪ A named SQL Server System Administrator login ID ▪ If Force protocol encryption is enabled: Microsoft Native Client
Microsoft SQL Azure	▪ Microsoft Windows Azure credentials ▪ Microsoft SQL Server Native Client
Oracle (9i and later, including Express)	▪ Oracle DBA credentials ▪ Oracle database drivers on all Agents connecting directly to the Datastore
IBM DB2 (9.1 and later)	▪ An existing database and a database user with access to a table space with a page size of at least 8k ▪ IBM DB2 OLEDB provider on all Agents connecting directly to the Datastore **Preparations for creating a Datastore on DB2** 1. Create a local user on the DB2 Server. This account will be used to connect to the RES Workspace Manager Datastore. 2. Manually create a database on the DB2 Server. 3. Create a Table Space for the user in the new database. Specify a buffer pool of 8KB. 4. Create a schema in the new database. 5. Add the new user to the new database. 6. Assign the applicable authorities, and add the schema and Table Space you created for this user. Make sure you assign the proper privileges.
MySQL (5.0 and later)	▪ MySQL DBA credentials ▪ MySQL ODBC driver on the database server and on all Agents connecting directly to the Datastore

5.2 Installing RES Workspace Manager and Configuring the Shell

The installation of RES Workspace Manager consists of two parts:

- Installing the product
- Configuring the **Workspace Composer** as the default shell

Installing RES Workspace Manager

The first step in setting up User Workspace Management is to install RES Workspace Manager 2014 on the computer on which you want to manage User Workspaces. With the installation of RES Workspace Manager 2014, the Management Console and an Agent will be installed.

- To install RES Workspace Manager 2014 Bronze, Silver or Gold license edition on your computer, use the **RES Workspace Manager Installer** (`RES-WM-Installer-2014.exe`).

- The **RES Workspace Manager Installer** is an installation package that contains the `.msi` files for the different components of RES Workspace Manager, grouped in one executable making it easier to install all necessary RES Workspace Manager components. When using the RES Workspace Manager Installer you can either **Select and install components** on the machine on which you are currently working or **Extract all components** for later use.
  - Choosing the option **Select and install components**, allows you to select which component(s) should be installed on the machine. The installation wizard of the selected component(s) will then guide you through the actual installation. The RES Workspace Manager Installer auto-detects whether the 64-bit or 32-bit version of the component(s) needs to be installed.

    You can install the following components:

    Clients: Workspace Composer
    Management Console

    Services: Relay Server
    Reporting Services

    Extra: Desktop Sampler
    Language Packs
  - When extracting all components, individual `.msi` files will be saved in the specified location.
- Instead of installing RES Workspace Manager, you can choose to perform:
  - a Console-only installation, if you do not want to install a RES Workspace Manager Agent on the computer on which you want to manage your environment (use `RES-WM-2014-Console.msi`).
  - an Agent-only installation, if you want to install RES Workspace Manager without a Console (use `RES-WM-2014-Agent.msi`).
    Please note that it is not possible to install a Console-only and an Agent-only installation side by side on the same machine. To go from a partial installation to a full installation, first uninstall the Console-only or Agent-only installation, then install the full RES Workspace Manager.

When installing RES Workspace Manager 2014, the Setup Wizard will guide you through the installation process.

- After reading and accepting the End-User License Agreement and specifying the installation folder, you will be asked whether you want the Workspace Composer to launch the next time someone logs on to the computer. If you have not yet created a Datastore, select **No, I will configure this later in the Management Console**. This option is not available for installations on Terminal Servers.
- After the installation of RES Workspace Manager 2014 has completed, the **Connection Wizard** will start. This wizard helps you to connect the installed Agent to an RES Workspace Manager environment.

Note

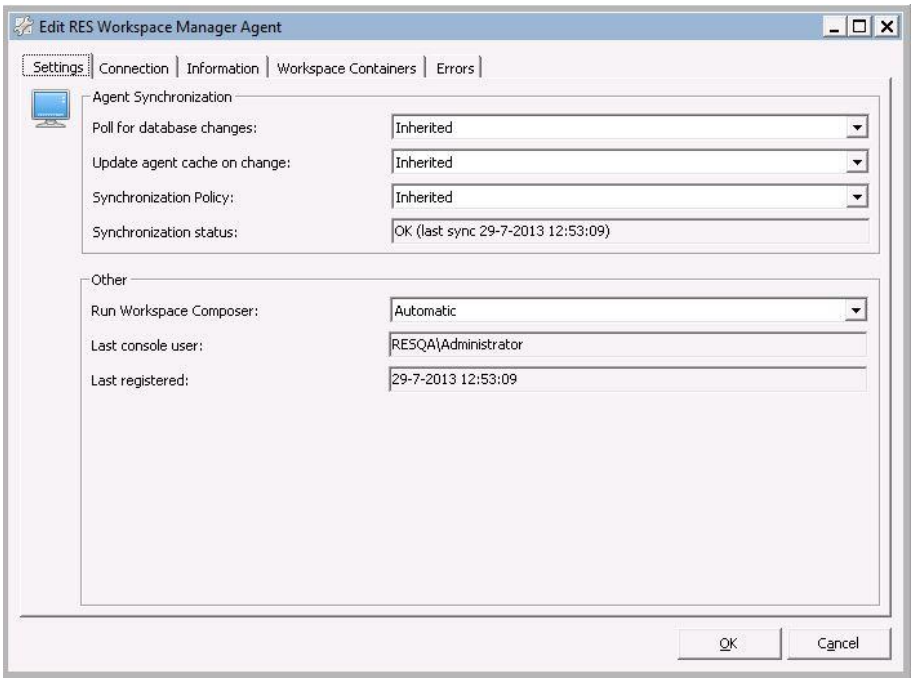
Installing RES Workspace Manager on a domain controller is not recommended as this may cause performance issues and unexpected behavior.

Configuring the Shell

To set the RES Workspace Manager Workspace Composer as desktop shell on a workstation, i.e. **desktops** and **laptops,** you need to configure that **pfwsmgr.exe** (the Workspace Composer) will start instead of the default **explorer.exe**. If you are installing RES Workspace Manager on a workstation, you will be prompted whether the Workspace Composer should run automatically when users log on to the workstation after completing the installation wizard. This option is only available for workstations (i.e. desktops and laptops). For Agents on servers or for specific users, it is still necessary to configure this manually. See **Centralized Computing** ("**Configuring the Shell - Centralized Computing**" on page 22).

If you choose not to run the Workspace Composer automatically after installation of the `.msi`, you may choose to change the shell later via the RES Workspace Manager Console at **Administration > Agents**.

The **Agents** node in the RES Workspace Manager Management Console, which gives an overview of the settings of all Agents in an environment, shows a column **Run Workspace Composer**. This column shows the value of the related setting on each Agent. The **Settings** tab of the **Edit RES Workspace Manager Agent** window, which is shown when editing the settings of a RES Workspace Manager Agent features the option **Run Workspace Composer**. This option, which is not available for Agents running on a server, makes it possible to choose whether the Workspace Composer should run automatically when a user logs on to the computer on which the Agent runs.



Setting the **Run Workspace Composer** option to **Automatic** sets specific registry keys. Of course it is also possible to set these values manually. Use the registry key located in:

`HKEY_LOCAL_MACHINE:SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`.

Edit the value "`Shell (REG_SZ)`" and set the data field to the location of "`pfwsmgr.exe`" (by default, this is `C:\Progra~1\Ressof~1\Worksp~1\pfwsmgr.exe`).

If you want a **user-specific** shell, you cannot use SetShell. You need to set the applicable registry keys manually. Use the registry key in:

`HKEY_CURRENT_USER:SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`.

Create a new value "Shell (REG_SZ)" and set the data field to the location of `pfwsmgr.exe` (by default, this is `C:\Progra~1\Ressof~1\Worksp~1\pfwsmgr.exe`).

5.3 Configuring the Shell - Centralized Computing

All users

If you use server-based computing and you want **all** users who log on using ICA or RDP to use the RES Workspace Manager Workspace Composer, you can use the **Terminal Services Configuration** tool to replace `explorer.exe` with `pfwsmgr.exe`. You can find this tool in the **Administrative Tools** folder.

FOR RDP:

It is possible to configure `pfwsmgr.exe` at the properties of a user in Active Directory, also at the Tab **Environment**.

In Active Directory you can also configure this in a GPO (Group Policy Object). Go to **User Configuration** > **Administrative Templates** > **System** > **"Custom user interface"**, and fill in the correct path to `pfwsmgr.exe`.

You can also configure pwrstart.exe on the RDP protocol at the tab **Environment** and fill in the path from pwrstart.exe (`%ProgramFiles%\RES Software\Workspace Manager\pfwsmgr.exe`) at **Start the following program when the user logs on**.

Warning

If you are using Windows 2008 and RemoteApps, you may want to reconsider this option, because `pfwsmgr.exe` will start every time a RemoteApp is started.

When using one of these options, RES Workspace Manager will start as the shell in a user session and the Windows Desktop will not be started.

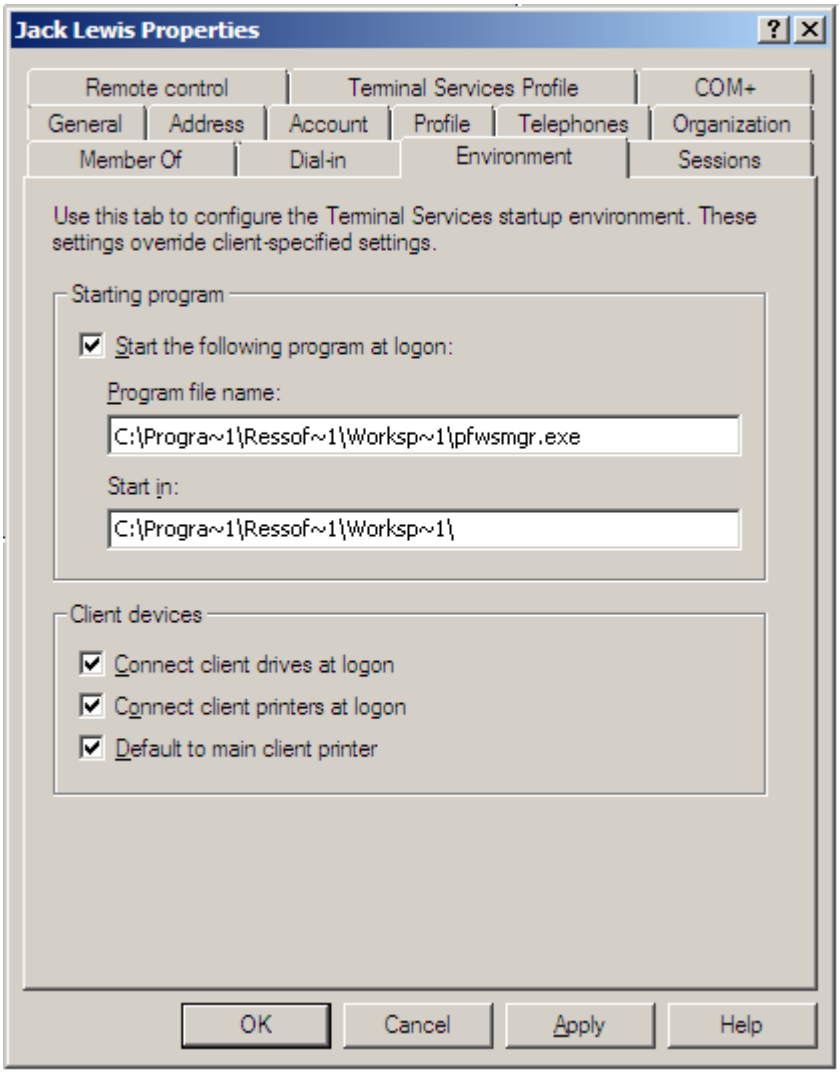
FOR CITRIX:

In AD you can also configure this in a GPO. Go to **User Configuration** > **Administrative Templates** > **System** > **"Custom user interface"**, and fill in the correct path to `pfwsmgr.exe`. This starts RES Workspace Manager when a user launches a Citrix Desktop.

Specific users

If you want to enable the RES Workspace Manager Workspace Composer for a specific user, use the **Environment** tab of the **User Properties** window. You can open this window in the **Active Directory Users and Computers** tool or in **User manager for NT Domains** on the server.

Configure `<path>\pfwsmgr.exe` as the startup application at logon. `<Path>` is the path where `pfwsmgr.exe` is located (by default `C:\Progra~1\Ressof~1\Worksp~1\pfwsmgr.exe`).



5.4 Setting up the Datastore

After installing RES Workspace Manager and optionally changing the Shell to the Workspace Composer, it is time to create a Datastore or to connect to an existing one. Because we are installing RES Workspace Manager for the first time, no Datastore is available yet.

When you start the RES Workspace Manager Console for the first time, you will be prompted whether to create a new Datastore or to connect to an existing one. Click the **Create** button to start the Datastore Wizard, which allows you to create a new Datastore.

When the process of creating the Datastore_ has finished, the RES Workspace Manager Console will restart and all nodes will be available.

The RES Workspace Manager Console

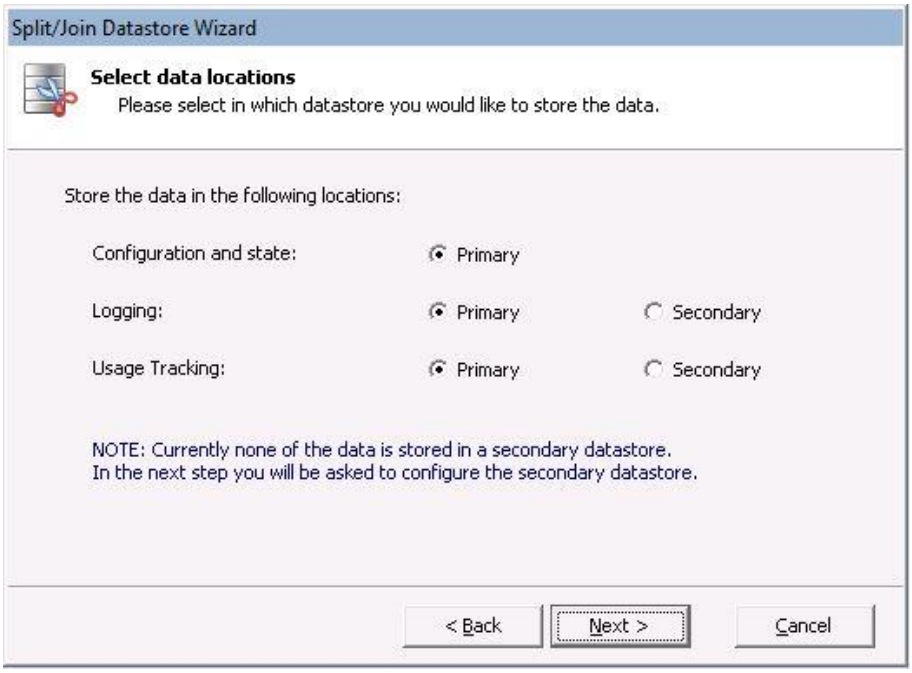
When RES Workspace Manager is installed, it is possible to manage this desktop from an external RES Workspace Manager Console. To do so, install only a RES Workspace Manager Console (not the full RES Workspace Manager) on your server by running the file `RES-WM-2014-Console-xxx.msi`.

When the installation is finished, connect to the existing Datastore that you created earlier. The Datastore Connection Wizard will guide you through this process. You will be able to manage the desktop installation of RES Workspace Manager from this location.

Store Usage Tracking and Log data in separate databases

It is possible to split the Datastore into two separate databases. The main database always contains Configuration and State data. The new database can contain either the Logging or Usage Tracking data or both. Because Logging and Usage Tracking data may cause very large database sizes, storing that data in a separate database can for instance allow the design of the database infrastructure to be more flexible when considering WAN scenarios.

A **Split/Join database wizard** is available that allows you to select a primary database and choose to split the current database and move Usage Tracking and/or Logging information into a new database or join already split databases.



Datastore Migration Wizard

The **Migrate** option makes it possible to migrate your existing RES Workspace Manager Datastore to a new type and/or location. This allows you to easily relocate your old RES Workspace Manager Datastore or to, for instance, migrate from a Microsoft SQL 2005 Datastore to a Microsoft SQL Azure Datastore. Migrations between all supported Database types are possible. All RES Workspace Manager Agents running RES Workspace Manager 2014 will connect to the new Datastore automatically.

For older RES Workspace Manager Agents you can optionally choose to automatically create a Building Block for a RES Automation Manager Module containing credentials and new database connection.

The final step of the wizard offers the option to transfer your RES Workspace Manager licenses to the new database. If you select this option the license activation of the old database will expire in 30 days. If you do not choose to transfer your licenses the new database gets no licenses but does get a new site ID.

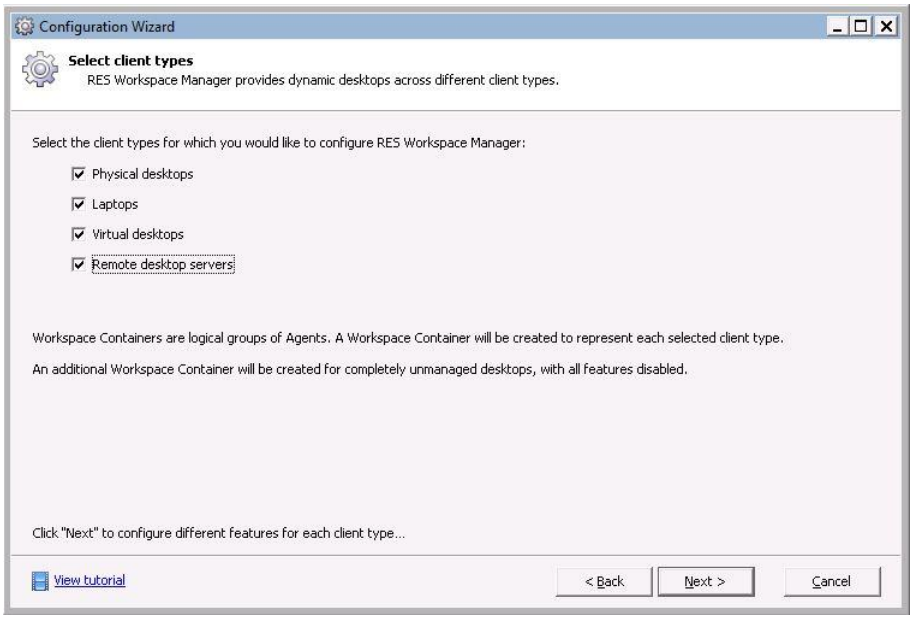
5.5 Configuration Wizard

The **Configuration Wizard** allows you to automatically add recommended configurations and example objects of various RES Workspace Manager functionality to your RES Workspace Manager site. This makes it easier to set up RES Workspace Manager sites.

After creating the Datastore, the **Configuration Wizard** will automatically start and guide you through setting up a basic configuration in RES Workspace Manager in a few easy steps. You have the choice to either create an **Evaluation** site or a **Production** site. Depending on this choice, two different routes for configuration can be followed.

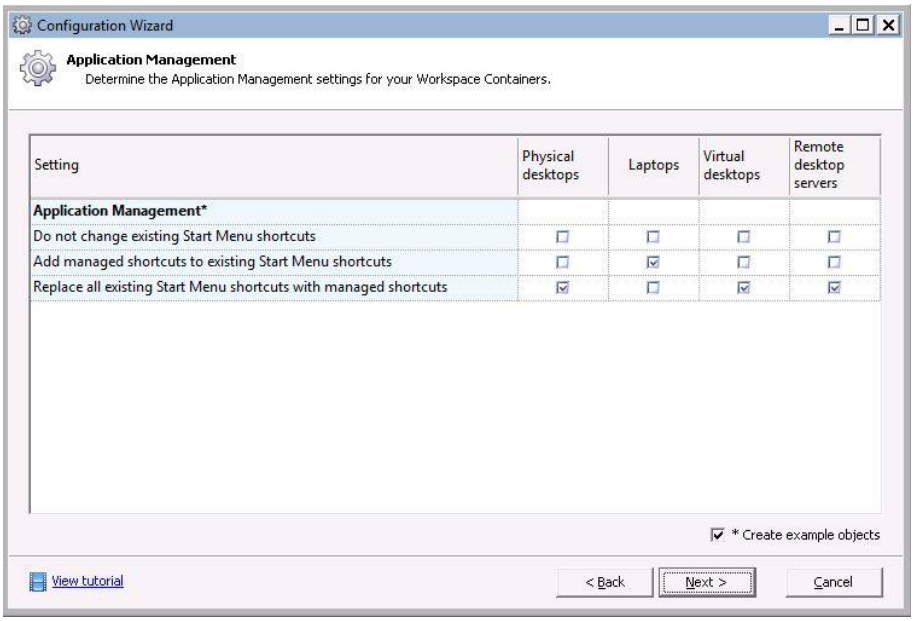
Creating an Evaluation site

1. When starting the configuration wizard, an introductory window welcomes you to the configuration wizard. You can either choose to view the online tutorial to be informed about the concept of workspace management or click **Next** if you are already familiar with our product.
2. You will be asked to select the type of RES Workspace Manager site you wish to create. Select **Evaluation**.
3. Select one or more Workspace Containers to create. Workspace Containers are logical groups of Agents. (for instance, physical or virtual desktops, laptops or remote desktop servers). At least one Workspace Container must be selected. Besides the Workspace Containers you selected, a Workspace Container "Unmanaged desktops" will be created, with all features disabled. The settings for the other Workspace Containers will be determined in the next steps of the wizard. If you want to know more about Workspace Containers click **View tutorial** or click **Next**.



4. Select the features you want to start using. Use **Ctrl + A** to (de)select all features. These features will be configured per Workspace Container. Click **Next**.

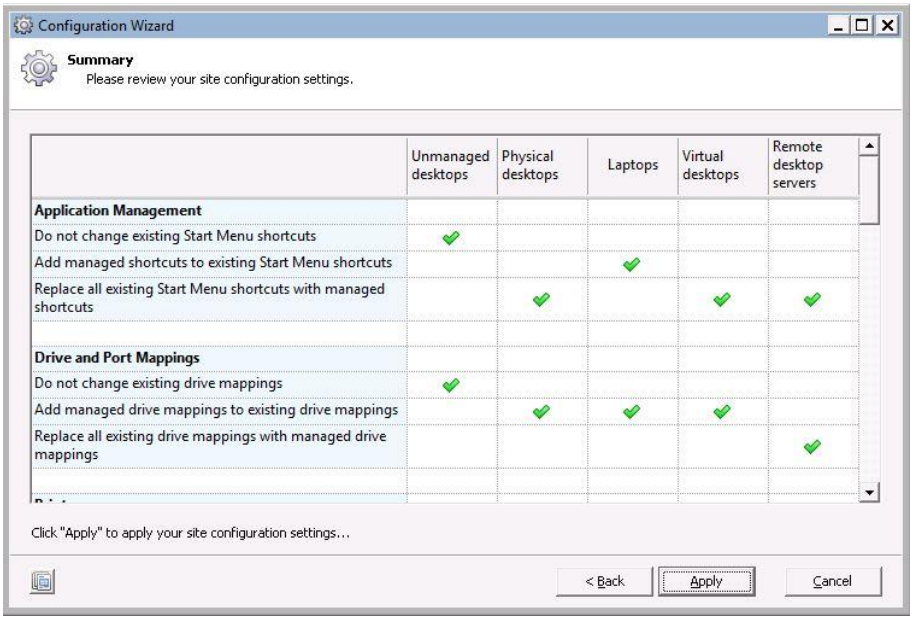
5. Specify the settings for each feature you selected in step 4. Most features can be enabled or disabled by selecting the relevant check box under the Workspace Container heading. If you want to create example objects for the feature you selected, select the check box **Create example objects**. Example objects are disabled by default when they are created. If you want more information about a specific feature (for example, Workspace performance or Application Management), click **View tutorial**. After you have specified the settings per feature (depending on your selection, you have to go through various windows), click **Next**.



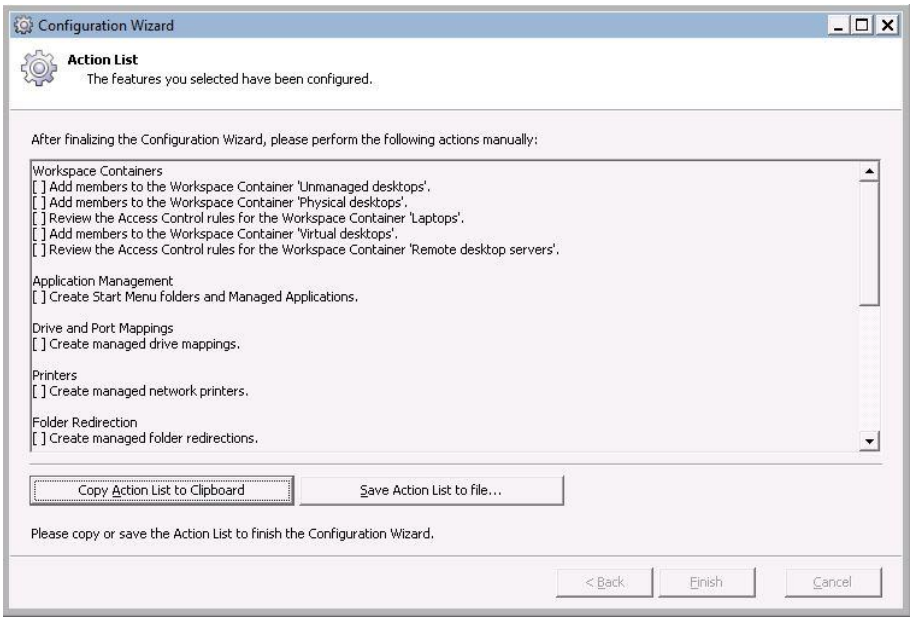
6. Additionally, the following example configurations (besides the example configurations you selected with the feature selection) can be selected:
   - Managed Applications
   - Settings executed at the start of a user session
   - An Administrative Role "Helpdesk"
   - Location-based printing

   Click **Next**.

7. Your site configuration settings are shown in a summary. You can click **Instant Report** to show and/or save the configuration wizard summary. If you want to change any of the settings click **Back**; if you agree with the settings, click **Apply**.



8. The configuration process will start, showing status and result information.
9. In the final step, you will see that the configuration has been completed. An Action List is shown, stating the items that still need attention after the wizard has finished. The Action List can be saved or copied on the clipboard. You can use the Action List afterwards as a reminder of the items you still have to configure. Click **Finish**.



After closing the configuration wizard, you will return to the top node in the Console: the Navigation map.

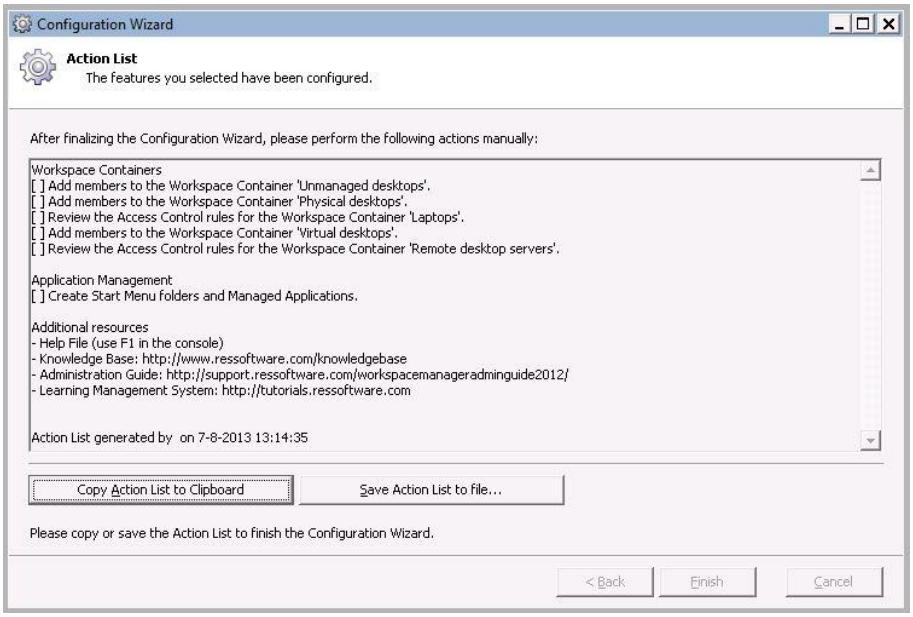
Note

If you click **Cancel** during any of the steps of the configuration wizard, the wizard will exit without changing anything in the configuration of the site. The next time the Console is started, the configuration wizard will start up automatically, as long as no configuration items have been saved.

Creating a Production site

1. When starting the configuration wizard, an introductory window will be shown welcoming you to the configuration wizard. You can either choose to view the online tutorial to be informed about the concept of workspace management or click **Next** if you already know our product.
2. You will be asked to select the type of RES Workspace Manager site you wish to create. Select **Production**.
3. The initial steps will be skipped and you can configure additional example configurations. Example objects are disabled by default when they are created:
   - Managed Applications
   - Settings executed at the start of a user session
   - An Administrative Role "Helpdesk"
   - Location-based printing

   Click **Next**.
4. Your site configuration settings are shown in a summary. You can click **Instant Report** to show and/or save the configuration wizard summary. If you want to change any of the settings click **Back**; if you agree with the settings, click **Apply**.
5. The configuration process will start, showing status and result information.
6. In the final step, you will see that the configuration has been completed. An Action List is shown, stating the items that still need attention after the wizard has finished. The Action List can be saved or copied on the clipboard. You can use the Action List afterwards as a reminder of the items you still have to configure. Click **Finish**.



After closing the configuration wizard, you will return to the top node in the Console: the Navigation map.

Tip

In the Summary (review site configuration settings) step of the configuration wizard, you can click the **Instant Report** button (not available in RES Workspace Manager Express Edition) to show or save the configuration wizard summary. You can use this summary as an overview or checklist which items and settings have been configured.

Notes

- To start the configuration wizard in a production site already containing configured items, click **Help > Configuration Wizard**. The steps will be the same as in **Creating a Production site**, except for step 2, which is skipped.
- The Console user needs the administrative role of "Technical Manager" with full rights to all nodes in RES Workspace Manager to be able to execute the Configuration Wizard.
- If you are using an **Express Edition** of RES Workspace Manager, only one Workspace Model will be created that you can configure (see step 3 of **Creating an Evaluation site**). In step 4, fewer features are available (Application Management, Drive Mappings and Network Printers, Profile Management (User settings) and RES Automation Manager). Also, the Administrative Role "Helpdesk" will not be created (see step 6 of **Creating an Evaluation site**). The other steps are the same.

5.6 Relay Servers

Relay Servers are an optional infrastructure component you can add to your site. As the Relay Server cannot create a Datastore, a valid Datastore must exist before one or more Relay Servers can be installed and configured. Next, the Agents can be set up to connect to the Relay Server instead of directly to the Datastore. It is also possible to have of mix of some Agents connecting to the Relay Server and others directly to the Datastore.

Relay Servers cache information from the Datastore and pass it on to Agents upon request, so that Agents do not need to contact the Datastore directly.

Installing and Configuring the Relay Server

Before installing a Relay Server, make sure you have an existing RES Workspace Manager Datastore. It is not possible to create a new Datastore during the installation of a Relay Server.

The first Relay Server in your environment must connect directly to the Datastore. Subsequent Relay Servers can connect to the Datastore or to parent Relay Servers.

The connections of a specific Relay Server are configured during or after installation of the Relay Server component. The behavior of Relay Servers, such as the interval at which they poll the Datastore for new information, is configured in the RES Workspace Manager Management Console at **Administration > Relay Servers**.

Warnings

- We do not advise installing a Relay Server on a machine that is also running an RES Workspace Manager Agent.
- The deployment of Relay Servers on 64-bit machines requires the installation of the 64-bit version of the necessary database drivers on these machines. The other components of RES Workspace Manager use the 32-bit version of these database drivers. It is not possible to use both versions on the same 64-bit machine simultaneously, so it is not possible to use a Console and a Relay Server on this machine that both point to the same Datastore.

Prerequisites

The following prerequisites apply to machines running the Relay Server component:

- Microsoft .NET Framework 4.0 or later.
- Any of the following server operating systems:

- Microsoft Windows 2003 x86/x64
- Microsoft Windows 2003 R2 x86/x64
- Microsoft Windows 2008 x86/x64
- Microsoft Windows 2008 R2 x64
- Microsoft Windows 2012 x64
- Microsoft Windows 2012 R2 x64

  - Available hard disk storage space must be at least 500 MB *plus* the current size of the Agent cache. (The size of the "Configuration and state" part of the primary Datastore provides an indication of the current cache size).
  - A Relay Server connecting directly to the Datastore needs to have the database client installed for the type of database used for the RES Workspace Manager Datastore. A child Relay Server connecting to another Relay Server does not need a database client.
  - An environment password must be configured in the RES Workspace Manager Console (at the **Relay Servers** node, using the button **Change environment password**). This secures your Relay Servers from unauthorized access.

Notes

The following operating systems are also supported, but these may set a maximum on the number of inbound connections:

- Microsoft Windows XP x86/x64
- Microsoft Windows Vista x86/x64
- Microsoft Windows 7 x86/x64
- Microsoft Windows 8 x86/x64
- Microsoft Windows 8.1 x86/x64

RES Workspace Manager only supports the ANSI version of the MySQL ODBC Driver 5.2.4.

Available installation methods

There are several ways to install the Relay Server component:

- Interactive installation with a wizard, followed by the Relay Server Configuration tool.
- Unattended installation followed by the Relay Server Configuration tool.
- Unattended installation, providing pre-defined connection settings in an XML file.

Regardless of the installation method, use the **RES Workspace Manager Installer** (`RES-WM-Installer-2014.exe`) to install the Relay Server.
When selecting the option **Select and install components**, the installation wizard will guide you through the actual installation. The RES Workspace Manager Installer auto-detects whether the 64-bit or 32-bit version of the Relay Server needs to be installed.
When selecting the option **Extract all components**, use the installation file `RES-WM-2014-Relay-Server(x64)-xx.msi` for 64-bit systems, or `RES-WM-2014-Relay-Server(x86)-xx.msi` for 32-bit systems.

During an interactive installation, the installation wizard automatically opens the Relay Server Configuration tool.

Unattended installation alone will not connect the newly installed Relay Server to any RES Workspace Manager environment. To configure this connection after the unattended installation, open the Relay Server Configuration tool.

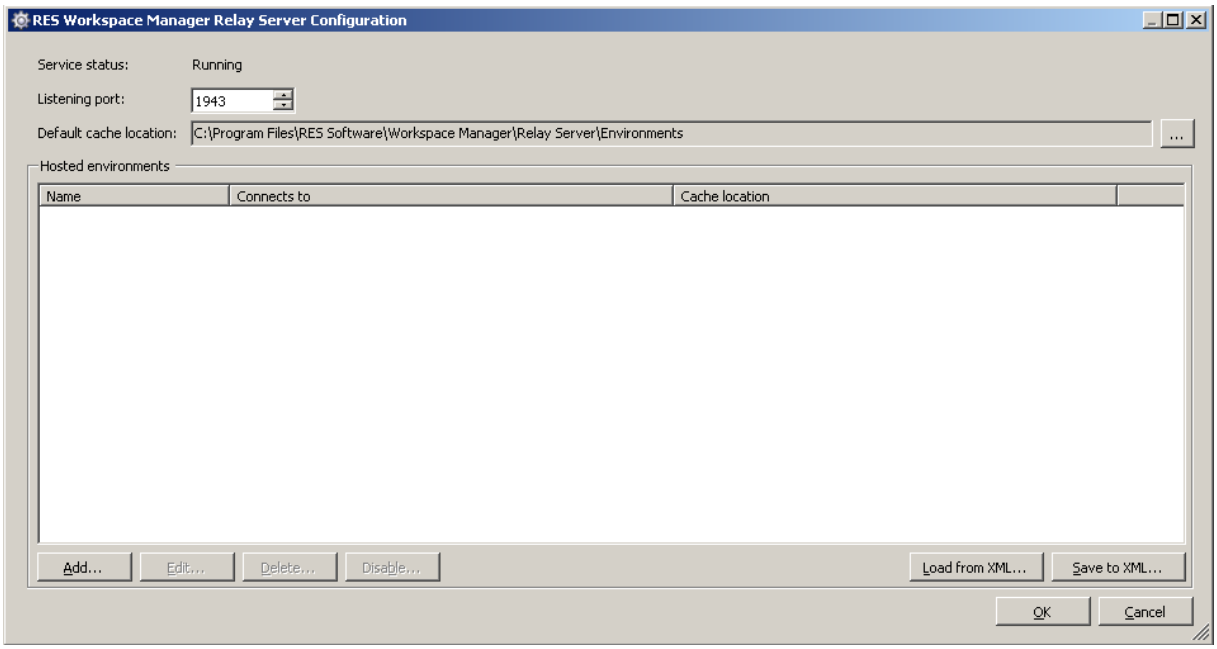
Alternatively, you can use the connection information previously configured for a Relay Server on a different machine. To do so, open the Relay Server Configuration tool on the configured Relay Server and click **Save to XML…**. For the unattended installation of a subsequent new Relay Server, ensure that the XML file is available on a local device (so not on a network share or mapped drive). In the command line for installation, provide the path to the XML file using the public property: `configfile=[path and file name]`.

For example:

```
msiexec /i c:\temp\RES-WM-2014-Relay-Server(x64).msi
configfile=c:\temp\rls.xml /qn
```

The Relay Server Configuration tool

Use the Relay Server Configuration tool to view and manage the Relay Server's connections to RES Workspace Manager environments.



On a machine running the Relay Server component, the Relay Server Configuration tool is available in the Start Menu. During interactive installation of the Relay Server component, the wizard automatically opens the Relay Server Configuration tool.

- Choose a **Listening port** that is not used by any other process on this machine.
- You can override the **Default cache location** per connected environment.
- Choose **Save as XML** to export the list of environments and their settings to an XML file that you can use later when installing another similar Relay Server.
- Choose **Load from XML** to import settings that you saved to XML when configuring a previous Relay Server. You can then edit the imported connection if necessary.

Connecting a Relay Server directly to the Datastore

The first Relay Server in a RES Workspace Manager environment must connect directly to the Datastore. The first Relay Server would normally be connected using the Relay Server Configuration tool. Other Relay Servers can connect directly to the Datastore or to other Relay Servers.

If you want to protect Relay Servers in your environment from unauthorized connections, please set an environment password first, *before* connecting the first Relay Server. The environment password is set (and can be changed) at the **Relay Servers** node in the Console.

To connect a Relay Server to the Datastore:

- Click **Add** in the Relay Server Configuration tool to open the **Relay Server Connection Wizard**.
- Follow the prompts in the **Relay Server Connection Wizard** to connect the Relay Server to the RES Workspace Manager environment.
- Choose **Datastore** as the connection type and provide information about the relevant Datastore.

Security Best Practice

When connecting the Relay Server to a Datastore on a Microsoft SQL Server using Windows Authentication, it is recommended to run the Relay Server Service with a **Windows account** instead of the **Local System account**. The Windows account that is used must be a domain account and needs the user right "Log on as a service".

Connecting a Relay Server to other Relay Servers

Instead of connecting directly to the Datastore, subsequent Relay Servers can also connect to parent Relay Servers. A parent Relay Server can have several child Relay Servers.

- Click **Add** in the Relay Server Configuration tool to open the Relay Server Connection Wizard.
- Follow the prompts in the Relay Server Connection Wizard to connect the Relay Server to the RES Workspace Manager environment.
- Choose **Other Relay Servers** as the connection type, then provide information about one or more parent Relay Server(s).
- Since each Relay Server can optionally host multiple environments, you also need to define the relevant environment. For easy reference, the correct environment name is shown in the **Relay Server** node in the RES Workspace Manager Management Console.
- Provide the environment password if one has been configured. (The environment password is set and changed in the RES Workspace Manager Management Console.)

Tip

For optimum security, we recommend that Agents connect to Relay Servers; and that Relay Servers with a Datastore connection use a service account (Windows credentials) and SQL encryption to connect to SQL Server.

5.7 Agents

Besides configuring the Shell, the **Agents** node also allows you to:

- View the **settings** of a specific Agent, including how it is identified in your environment
- Configure when local caches on Agents are **updated**
- Determine the **Datastore connection** an Agent uses and how it uses this connection

On the **Settings** tab of **Administration > Agents**, the global settings for Agents can be configured. On the **Agents** tab, all connected Agents are shown. By clicking **Edit** in the command bar, settings for individual Agents can be changed. Here you also configure if the Agent connects to the Datastore or Relay Servers; and if the latter, you can configure how Agents determine which Relay Server to use.

Poll for database changes

All configuration data in the Datastore is cached to the Agent. Because most RES Workspace Manager components use this cached data instead of directly connecting to the Datastore, this significantly reduces the load on the central Datastore and eliminates it as a single point of failure in a RES Workspace Manager environment.

The local cache is kept up-to-date by the RES Workspace Manager Agent Service, which is also responsible for uploading log and Usage Tracking information to the Datastore/Relay Server. If a connection to the Datastore/Relay Server is not available, all log and Usage Tracking information will be cached locally until the connection is re-established.

The setting **Poll for changes** determines the interval at which Agents check whether they need to download any configuration changes, but also whether they need to execute any tasks. A longer polling interval means that it takes longer before Agents execute tasks such as remote publishing to Citrix XenApp servers, forcing a session refresh, restoring User Settings from the RES Workspace Manager Console, sending messages to users, and disconnect, log off and reset users.

The setting **Poll for changes** can be configured at global level (applies to all Agents) and for individual Agents (by editing the **Settings** of an Agent):

- **Every <period>**: polling the database will occur at the selected interval. A longer polling interval decreases the traffic on your network, but delays the execution of tasks and lengthens the time during which Agents are not aware they need to update their cache in order to reflect any changes in the Datastore.

Update Agent cache on change

The time span set at **Update Agent cache on change** determines the timing for Agents to actually download data and update their cache. A short interval may result in many Agents starting to download data at the same time. A long interval will spread the network load more evenly, but as a result it will take longer before all Agents reflect the necessary changes.

Update Agent cache on change can be configured at global level (applies to all Agents) and for individual Agents (by editing the **Settings** of an Agent):

- **Immediately**: each Agent will update its local cache as soon as it the Poll for changes mechanism detects a relevant change in the Datastore. If many Agents detect changes at the same time, they may all start downloading data at the same time.
- **Within <period>**: the update of the local caches will be randomized and spread out over the selected period. Although this decreases the traffic on your network, it also means that the local caches on your Agents will not immediately reflect any changes in the Datastore.

You can also update Agent caches immediately from the context menu.

Synchronization policy

The synchronization policy of RES Workspace Manager determines what should happen if the synchronization of an Agent fails. The policy that you select will first be applied when you click **Apply**. The setting **Synchronization policy** can be configured at global level (applies to all Agents) and for individual Agents (by editing the **Settings** of an Agent):

- **Abort on error**: the synchronization process will be aborted if the synchronization of an Agent fails (for example, because it is not possible to update the local cache or because an error occurs). If this happens, you first have to correct the cause of the failure before the synchronization of the Agent will be successful again. This option is selected by default.
- **Continue on error**: the synchronization process will continue, even if an error occurs.

If a synchronization fails, RES Workspace Manager will attempt a new synchronization after minimally one hour, irrespective of the synchronization policy that you specified.

Identify Agents by

By default, Agents are identified by Computer domain name and NetBIOS name. At **Identify RES Workspace Manager Agents**, select a different method of identification if:

- the operating system is re-installed on Agents.
- several virtual machines use the same image.
- several computers are deployed using imaging.

Datastore connection

You can configure the default behavior of Agents: **Connect directly to the Datastore** or **Connect through Relay Server**. If they should connect to relay servers, you can select the **Connection method(s)**:

- **Discover**: Relay Servers in the environment will be discovered automatically
- **Randomly from List**: Relay Servers will be selected according to the provided list. The Relay Servers can be entered manually or previously discovered Relay Servers can be selected from the list.
- **Fallback to FQDN**: an FQDN can be provided to which Agents can fall back if the other options fail**.**

These connection options do not exclude one another and can be used in combination.

Run Workspace Composer automatically

You can configure Agents to run the Workspace Composer automatically from the context menu, and by editing the **Settings** of an Agent:

- **Automatic**: the Workspace Composer will run automatically when users log on.
- **Manual**: users need to start the Workspace Composer manually (for example, from the Start Menu).

These settings are reflected in the **Run Workspace Composer** column in the Agents list. If the column shows the value **Automatic (pending)** or **Manual (pending)**, the Agent cache has not been updated yet.

- This field is unavailable for Agents running on Terminal Servers. See the **RES Workspace Manager Administration Guide** for information about the configuration of this feature for Terminal Servers.
- For Agents running on Citrix XenApp special considerations apply. See the document **Migrating Existing Citrix XenApp Published Applications to RES Workspace Manager**, where various scenarios are explained, depending on whether you want to republish your existing Citrix published applications or want to manage them using the Intercept option **If managed shortcut was not used**. The setting **Run Workspace Composer** of the Agent must be configured according to the scenario you choose. The workings of the Intercept option are discussed in the section **Composition, Application Properties, General** of this Administration Guide.

Workspace Container membership

You can configure membership of Workspace Containers of Agents at **User Context > Workspace Containers**, but also by editing the **Settings** of an Agent.

Deleting Agents

Deleting Agents can be useful if Agents have become obsolete or if they, for some time, fail to synchronize with a Datastore in your environment. If you delete an Agent, but it manages to re-establish a connection to a Datastore in your environment, it will automatically be included again in the list of Agents.

Notes

- The **Agents Overview** node shows a read-only overview of all Agents and their settings.
- If you use identification method MAC address of the first enabled network interface and an Agent has multiple network cards, RES Workspace Manager will use the MAC address of the first enabled network card, based on the order as defined on the agent by Microsoft Windows. You can find this order in Microsoft Windows by clicking **Start > Settings > Network Connections > Advanced > Advanced Settings**.
- The **FQDN** column displays the Fully Qualified Domain Name, once the option **Use computer's FQDN instead of domain\computername in Logs and Usage tracking** has been enabled at **Advanced Settings** in the **Setup** menu.
- The columns **AppGuard version**, **NetGuard version**, **RegGuard version** and **ImgGuard version** in the **Agents** node and **Agents Overview** node show the internal driver versions that RES Workspace Manager uses. These version numbers can be used for troubleshooting purposes, should issues arise in your environment following an upgrade or downgrade or after installing a fixpack.
- The **Synchronization status** column in the **Agents node** and **Agents Overview** node shows when the last synchronization of an agent took place and whether this was successful. If a synchronization fails, RES Workspace Manager will attempt a new synchronization after minimally one hour, irrespective of the synchronization policy that you specified.
- Licensing information is always updated immediately, irrespective of the settings that you specify.
- When using Relay Servers, we recommend creating separate Workspace Containers for each subsite with different Relay Server lists. This way, it is easy to identify to which Relay Server an Agent or group of Agents normally connects.
- An Agent can connect directly to the Datastore OR it can use Relay Servers.
- An Agent configured to connect to Relay Servers will never connect to the Datastore directly. If it cannot connect to a Relay Server, it will use information stored in its local cache. An Agent configured to connect to the Datastore directly will never connect to Relay Servers. If its connections are not available, an Agent will use information stored in its local cache.
- All Agent-related errors are also visible on the **Errors** tab of a specific Agent.

5.8 RES Workspace Manager Licensing

When RES Workspace Manager is installed, an evaluation license for **25 Named Users** for RES Workspace Manager is made available automatically, as well as an evaluation license for RES VDX for **25 VDX clients**. Evaluation licenses are valid for 45 days.

During the evaluation period, you can try out the different sets of functionality that RES Workspace Manager editions offer, by switching between the different RES Workspace Manager Editions. See **RES Workspace Manager modules** (on page 45).

When the evaluation period expires, RES Workspace Manager will automatically switch to the Express Edition. To continue using other modules of RES Workspace Manager, you need to use the licenses purchased from your reseller.

5.8.1 Licensing Model

Licenses are pooled per environment and are claimed by RES Workspace Manager Agents according to the rules outlined below.

Named User licenses

When using Named User licenses only, the following applies:

- All users will claim a Named User license upon first session connect. Once the license is claimed, the user is allowed to use any type of client (Terminal Server, desktop or laptop) with the assigned user account.
- An offline laptop will only allow the logged-on user to use RES Workspace Manager.

Licensing information is stored in the Datastore and cached locally on Agents. If, according to the local cache, licenses are available for the session, the session is allowed. If, according to the local cache, no licenses are available, the RES Workspace Manager licensing policy is applied.

See **Managing Licenses** (on page 43) for information about how to set up a licensing policy.

Concurrent licenses

When using Concurrent licenses only, the following applies:

- RES Workspace Manager claims a concurrent license for each active workspace (regardless of user name, client name or computer name).

Each laptop claims a seat, regardless of user sessions or Datastore connection state. A license claimed by a laptop will remain claimed whether anyone uses the laptop or not. A laptop can only claim a license when one is available.

Combining Named User licenses and Concurrent licenses

Concurrent licenses can be used alongside Named Licenses. Concurrent licenses are based on the number of simultaneous User Workspace sessions. When using Concurrent licenses and Named Licenses together, the following applies:

- If a Named User license has already been claimed or reserved for the user who is logging on, this license will be used.
- If no license is claimed/reserved, RES Workspace Manager checks whether the current device is a laptop.
- On laptops, RES Workspace Manager first tries to claim a Named User license. If no Named User license is available, it will try to claim a Concurrent license.
- On other types of devices, RES Workspace Manager first tries to claim a Concurrent license. If no Concurrent license is available, it will try to claim a Named User license.
- If no license can be claimed, the RES Workspace Manager licensing policy is applied.
- If you use several published applications, you only need a license for the first session originating from the same client - even if the sessions run on different servers and the client has no composer running. Prerequisite is that all sessions run using the same database.
- If the originating client uses a local composer, it already has a license in use - any subsequent remote session will not require a license, even if different databases are used.

Named or Concurrent?

RES Workspace Manager offers two license types: Named User licenses and Concurrent licenses. Which license type, or combination of licenses you need, very much depends on the number of users, Workspaces and devices in your environment. Concurrent licensing is mainly used in Virtual Desktop environments and Named licensing for mobile workers (laptops). For example, when a user works on a laptop and connects to a Virtual Desktop, a Named User license suffices to work with RES Workspace Manager on both, as the license is associated to the user name.

It is possible to mix Concurrent and Named users in one RES Workspace Manager environment, but both licenses need to contain the same modules. It is not possible to use different modules for different (groups of) users. For example, for mobile workers (laptops) the Dynamic Configuration module and for XenDesktop users the Dynamic Configuration, Delegation and Compliance, and Adaptive Security modules. In this case, every user needs all three modules.

The following examples illustrate a number of environments with their most advantageous license types:

Laptops

Case	Why?
▪ 1000 users: 800 laptops, 200 desktops ▪ 1000 Named licenses	▪ Users are bound to a device, so Named is cheaper.

Desktops

Case	Why?
▪ 1000 users: 600 desktops ▪ 600 Concurrent licenses	▪ Less Workspaces than users, so Concurrent is cheaper.

Terminal Services

Case	Why?
▪ 2000 users: 1200 Workspaces at a time ▪ 1200 Concurrent licenses	▪ Less Workspaces than users, so Concurrent is cheaper.

Terminal Services and Laptops (1)

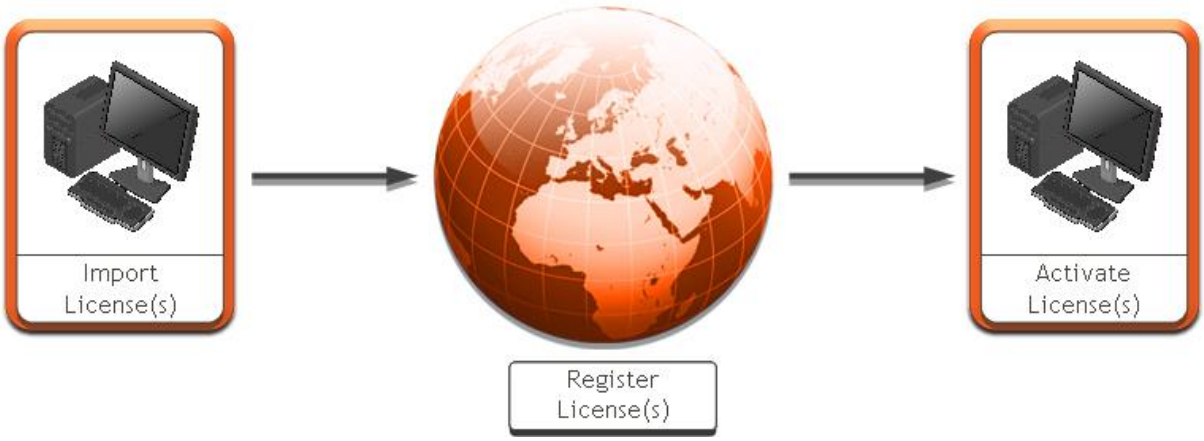
Case	Why?
▪ 800 users: 800 laptops offline, that use Terminal services in the office ▪ 800 Named licenses	▪ Users are bound to a device, so Named is cheaper.

Terminal Services and Laptops (2)

Case	Why?
▪ 1200 users: 400 laptops, 800 Workspaces ▪ 400 Named licenses + 400 Concurrent licenses	▪ Different kinds of usage. Mobile workers that use Terminal Services in the office are better off with Named, but the other 400 active sessions are better off with Concurrent. ▪ Reserve Named User licenses for laptop users!

5.8.2 Licensing Process

In RES Workspace Manager licenses need to be imported, registered and activated, using the **License Wizard**.



Step 1: Import all licenses

1. Save the license file that you received by e-mail to an accessible location.
2. Open the **License Wizard** and select **Add RES Software license**.
3. Follow the prompts to import the license(s) to the Datastore. All new licenses should be imported at the same time.

4. At the end of the process, you will be prompted to activate your license(s).
   - Evaluation licenses and Corporate licenses need to be activated immediately.
   - Production licenses need to be activated within 30 days, after which they expire.
5. When you have completed the import process, your licenses and all relevant information will be shown in the **Licensing** node.

Step 2: Register and activate the licenses

When you have imported all your licenses, start the License Wizard. RES Workspace Manager will scan for any license that has not been activated and activate all of them at the same time. The Site ID will be activated automatically when you activate your licenses: it does not need to be registered separately.

1. In the **License Wizard** select **Register and automatically activate RES Software license(s)**.
2. Follow the prompts to register and activate your licenses.
   - The name of your site links your licenses to your business and must therefore be a unique name.

   In certain situations, automatic activation of licenses is not possible. In these situations, follow the prompts to activate your license(s) manually. The information is stored in a text file that you can send to RES Software:

   - **Web**: e-mail the activation request from the RES Software website.
   - **E-mail**: e-mail the activation request to RES Software directly from an e-mail client on the computer running the Console (requires a configured MAPI-compliant e-mail client).
   - **Save to file**: save the activation request as a text file that you send to activation@ressoftware.com.

   Within 24 hours during workdays, RES Software will send an activation file to the mail recipient that you specified. Save the activation file to an accessible location, open the **License Wizard** and select **Import activation file for RES Software license(s)**.

When you have activated your licenses, the **Licensing** node will display an overview of your licenses, including license type, RES Workspace Manager edition, site and license status and the number of licenses that are available and claimed. The active RES Workspace Manager Modules are also displayed on this node.

Warning

License files and activation files contain crucial information. **Do not edit these files, because it will render them useless**.

Notes

- If you import any additional licenses at a later stage, they can be registered and activated using the procedure as described above. Additional licenses must be registered under the same Site name.
- Licenses that are deleted and then added to the Datastore again also need to be activated again.
- After completing the licensing process, the default Site ID is automatically replaced by a true Site ID that links your licenses to your business.
- Adding an RES Workspace Manager Silver license edition to an RES PowerFuse Standard license will result in **Silver** edition.

Tips

- The RES Software Portal at http://support.ressoftware.com provides Solution Assurance benefits and access to product support. The portal is available to registered customers with valid, activated licenses.
- To register your company, visit http://support.ressoftware.com and enter the Site ID of your environment.

5.8.3 Managing Licenses

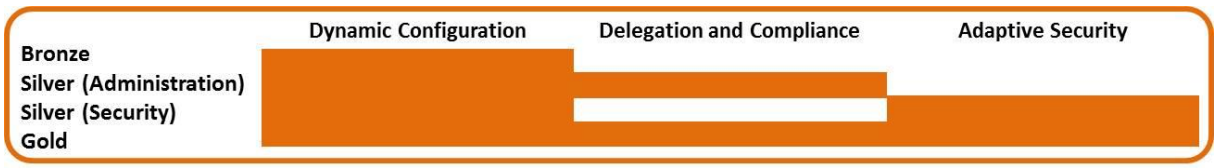
You can manage your licenses in the Console at **Setup > Licensing**.

- Evaluation licenses are valid for 45 days. During this period, you can try out the different sets of functionality that RES Workspace Manager modules offer, by switching between the different RES Workspace Manager modules. To switch to a different RES Workspace Manager module, click the **Module(s)** link and select a choice in the **Licenses evaluation** window.
- To obtain (additional) licenses, click **Get Licenses**. This opens a web page with contact details of your nearest reseller. Alternatively, when evaluating RES Workspace Manager Express Edition, click **Get Free Licenses**. This opens the Express License Wizard, which allows you to obtain a free Express Edition license for an unlimited number of users and without expiration date.
- To view the details of a license, click **View**. You can only view the details of non-evaluation licenses.
- To delete a license, for example because they have expired, click **Delete**. You can only delete non-evaluation licenses.
- To import, register and activate RES Workspace Manager licenses, click **License Wizard**. You can also use this wizard for RES VDX licenses (not available when using RES Workspace Manager Express Edition).
- To set up a licensing policy, use **If no license available at logon**. A licensing policy specifies what should happen if no license is available when a user starts a workspace session. This option is only available when using RES Workspace Manager Gold, Silver or Bronze license editions.
- **Continue with limited functionality**: When selected and no licenses are available when a user logs on, a message will be shown to the user: "There is no license available. RES Workspace Manager will start a restricted session that offers only limited functionality. Please contact your administrator." When selecting this option, the user can still log on, but only Express Edition functionality will be available. The event of no available licenses will also be logged in the Event log with an exclamation mark.
- **Continue with reminder for 45 days**: When selected and no licenses are available when a user logs on, the user can still use RES Workspace Manager full functionality for 45 days, but a message is logged in the User Event log and in the Error log that no license was available. Then, a countdown is started and if, after 45 days, there is still no license available, the user will not be able to start any session, until additional licenses have been added. In a new site, **Continue with reminder for 45 days** will be the default setting.
- **Do not continue, log off**: When selected and no licenses are available when a user logs on, a message will be shown to the user: "No RES Workspace Manager license available for session" and the user will be logged off automatically.
- When using Named User licenses, the **Named Users** tab is available. On this tab, you can view a list of all Named User licenses that are in use in your RES Workspace Manager environment and manage this type of license.

- Click **Reserve** to reserve a license for a specific named user. Once a license is reserved, it will remain reserved until released. Reserved licenses that are not claimed within 45 days are automatically released after this period. When reserving a Named User license, please take into account that an Agent must come online in order to obtain information about this reservation. If the relevant user logs on to an Agent that has not been online since the license reservation was made, the license reservation will not take effect.
- To release a reserved license, select it and click **Release**. Releasing a license is useful if the number of available licenses is insufficient. If some licenses are reserved for named users, but never claimed (e.g. because someone is on holiday for three weeks), you can release these licenses again and make them available for other users.
- When using Concurrent licenses, the **Concurrent Users** tab is available. On this tab, you can view a list of all concurrent licenses that are in use in your RES Workspace Manager environment.

5.9 RES Workspace Manager modules

The RES Workspace Manager product family consists of different modules in which different sets of RES Workspace Manager 2014 features are available to different levels:



In RES Workspace Manager, the number of modules selected determines the license edition:

- The **Dynamic Configuration** module is the baseline module that is always included in any RES Workspace Manager license edition. The **Bronze** license edition consists of this single module.
- **Delegation and Compliance** and **Adaptive Security** are optional modules that offer additional sets of features. Selecting one of these in addition to **Dynamic Configuration** results in the **Silver** license edition. Selecting both results in the **Gold** license edition.

Dynamic Configuration module

Makes it possible to create a personalized (dynamic) desktop. The first step towards IT as a Service.
Users are provided with a context-aware and centrally managed workspace that contains all of the right applications, data, printing and personal settings essential for their productive working. It contains the following technologies:

- Desktop Transformation
- Application Management
- Zero Profile Technology
- Workspace Analysis
- Folder Synchronization
- E-mail Settings

Delegation and Compliance module

Provides all the information to get insight of what is configured, changed, and used. The second step towards IT as a Service.
Provides administrative insight to improve your ability to manage your infrastructure with clear logs of changes, current status reporting, and license usage data from all users. Plus, it supports administrators in managing different application delivery techniques, which includes presentation and application virtualization. It contains the following technologies:

- Delegation of Control
- Remote Application Integration
- Alerting
- Instant Reporting
- Compliancy
- Tracking and Reporting
- Workspace Branding

Adaptive Security module

This is the third and last step towards IT as a Service.
You will be able to deliver a personalized desktop according to company business rules and compliance. Unauthorized actions such as executing certain applications and the use of removable disks are prevented based on the user's context. It contains the following technologies:

- Removable Disk Control
- Application Access
- Network Security
- User Installed Applications
- Locations and Devices
- Dynamic Privileges

For more details, please check the RES Workspace Manager Module Comparison Chart on http://www.ressoftware.com at the **Resources** section.

Notes

- All modules are fully compatible. Additional functionality is enabled through license keys, so that upgrades to other modules require no downtime or additional software deployment.
- During the evaluation period, you can simply switch between modules (at **Licensing** in the **Setup** menu). You can also switch if you have extended your evaluation period by importing evaluation licenses, or if you have NFR licenses (RES Software partners only).
- If you use a license edition other than Gold, unavailable features are masked in the Console by a brief description of that feature. To hide unavailable sections altogether, go to **Options** in the menu item and clear **Show unavailable features**. Alternatively, select **Do not show unavailable features** in one of the masked nodes. To include unavailable features in the view, select **Show unavailable features** again (in the **Options** menu item).

5.10 Directory Services

Having installed RES Workspace Manager on the desktop machine, we need to configure Directory Services at the **User Context > Directory Services** node of the RES Workspace Manager Console. The directory services used in your organization are the basis for your RES Workspace Manager environment: RES Workspace Manager delivers applications and resources based on the user, OU and group information that it retrieves from the directory services listed.

A directory service is used to store information about resources (such as printers), services (such as e-mail) and users in a network. The directory service provides information on these objects, organizes them, and provides authentication and validation. A well planned and well maintained directory service reflects the hierarchical and functional structure of an organization and is a powerful tool in the delivery of applications and resources to users.

RES Workspace Manager can retrieve information from:

- **Microsoft Windows Domains** (also called NT Domains)
- **Microsoft Active Directory Services** (also called AD or ADS)
- **Novell Directory Services** (also called NDS)
- the **local computer**

The Primary Domain of the Agent will be configured by default. However, you can use multiple directory services concurrently. This makes it possible to use RES Workspace Manager for specific parts of your IT environment. This can be particularly useful in very mixed environments, in environments where different administrators manage different sections, or if you wish to introduce RES Workspace Manager gradually rather than all at once.

For example, you can:

- configure a RES Workspace Manager Directory Service for tree A, and one for tree B, but not (yet) for tree C.
- configure a RES Workspace Manager Directory Service for a part of an Active Directory or Novell tree (by setting a mount point).
- use several Active Directory forests in one RES Workspace Manager environment.
- combine different parts of several Active Directory forests, plus a number of Microsoft Windows Domains.

Configuration

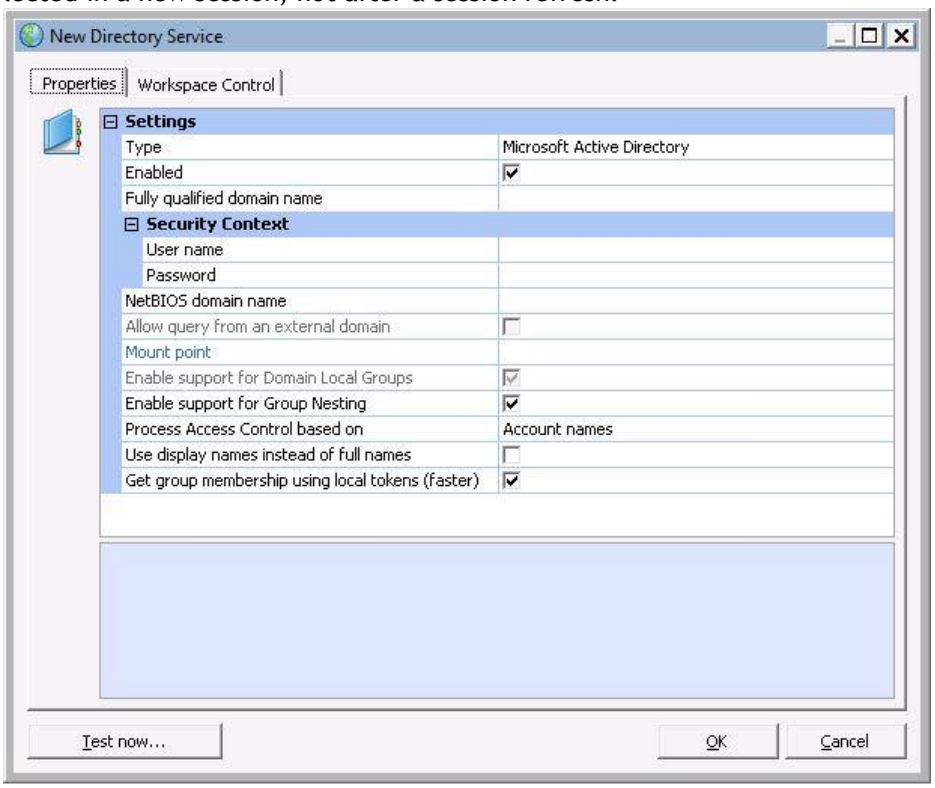
- RES Workspace Manager will use your environment's name resolution mechanism to resolve the selected **Fully Qualified Domain Names** to the correct paths.
- When configuring a Security Context:
- the account must be in the same domain as the directory service you are configuring.
- the account requires sufficient rights to query the domain in Active Directory or in Microsoft Windows Domain.

  These credentials will only be used when viewing data in the Management Console.
- If your environment does not include trusted domains, *not* **allowing query from external domains** will make sessions start up faster.
- With a **Mount Point**, objects in the tree above the mount point cannot be used in the Management Console unless another directory service starts in the same tree at a higher point.

- **Group Nesting** determines whether Access Control based on a parent group also applies to members of a subgroup. For example, suppose that Access Control for an application depends on membership of the group "AppUsers", and that this group contains the subgroup "AppAdmins".
  - *Without* support for group nesting, users must be member of the group "AppUsers" in order to get the application. Users who are only member of the subgroup "AppAdmins" do not get the application.
  - *With* support for group nesting, users who are only member of the group "AppAdmins" also get the application.
- You can select the method of resolving users and groups:

  Account names is preferable if user and group names do not change often. Renamed users and groups lose their current access because RES Workspace Manager cannot find a match for their name. This method is recommended if Building Blocks are used to transfer objects from test to production environments, since names then are the same, but SIDs are not.

  Account SIDs is preferable if user and group names change frequently. Account SIDs generally are considered safer, but less legible than account names. If a user or group is renamed, the account name changes but its SID does not. With Access Control based on SID, renamed users and groups keep their existing access and the RES Workspace Manager Console reflects their new names. Please note that when using this method, any changes in a user's group membership (and therefore Access Control based on this information) will first be reflected in a new session, not after a session refresh.



- Selecting the option **Get group membership using local tokens (faster)** for a directory service, the RES Workspace Composer will resolve the user's group membership from its logon token. This option is especially interesting for multi-domain environments, in which resolving cross domain group membership does not work properly or causes performance degradation.

Notes

- Any change in the user's group membership will only be effective after the user logs off and on again. A refresh of the user workspace will not suffice.
- The option **Get group membership using local tokens (faster)** should only be used in environments that have a Global Catalog server.
- It is advised to enable this option for all defined directory services in the RES Workspace Manager Console.

- In some situations, the order in which Directory Services may be important. When a user starts a session, RES Workspace Manager starts at the top of the list of Directory Services configured in the RES Workspace Manager Console. The first configured Directory Service that matches the user's logon domain becomes the primary directory service for the session.

  The following order is usually advisable:
  - all Active Directory Directory Services
  - all Microsoft Windows Domain Directory Services
  - the Local Computer Directory Service

  In complex environments, you may need to experiment with this order.

5.10.1 Novell Directory Services

At **User Context > Directory Services**, directory services can be configured. RES Workspace Manager delivers applications and resources based on the user, OU and group information that it retrieves from the directory services listed.

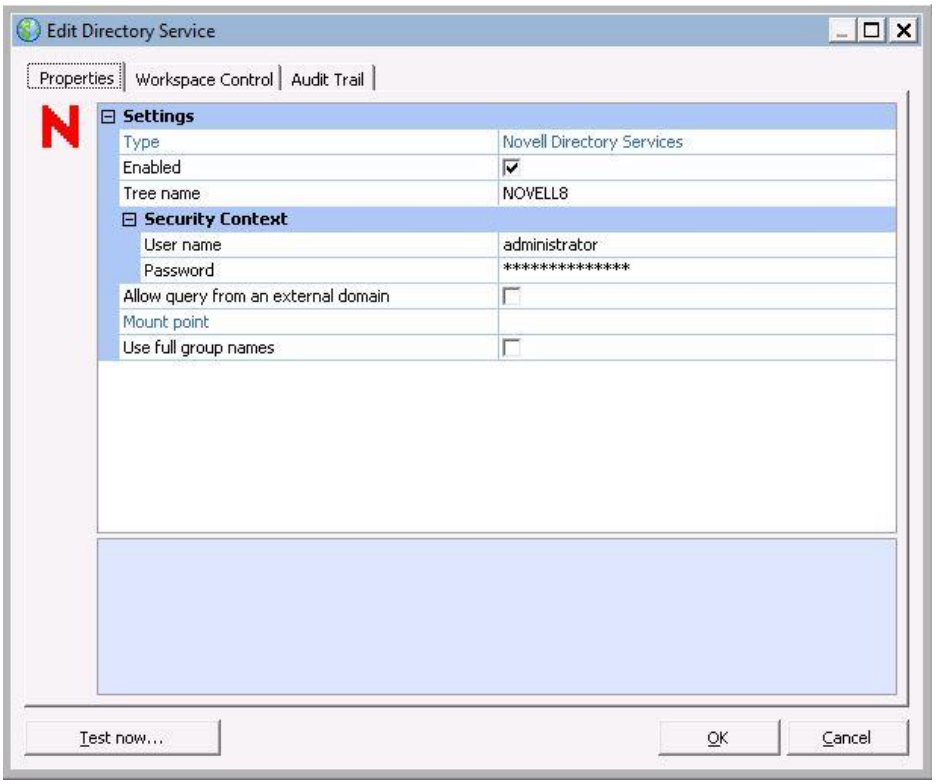
The following instructions apply specifically to Novell Directory Services:

Order of Directory Services

When a user logs on to a computer using the Novell Client, the Novell Client silently also logs that user on to a Microsoft Windows domain, or creates a new local user for this purpose. The way in which this is set up in your environment influences the identification of the user for the purposes of RES Workspace Manager:

- If the Novell Client also logs the user on to a Windows domain, and you have also listed a RES Workspace Manager Directory Service that includes that same domain, then you must place the Novell Directory Service higher in the list than the domain Directory Service. (Otherwise RES Workspace Manager will find the user in the other Directory Service and will not check the Novell Directory Service anymore.)

- If the Novell Client also logs the user on as a local user, and you have also listed a Local Computer Directory Service in RES Workspace Manager that will apply to the computer on which the user is logging on, then you must place the Novell Directory Service higher in the list than the local computer Directory Service. (Otherwise RES Workspace Manager will find the user in the other Directory Service and will not check the Novell Directory Service anymore.)



Group Names

In Novell Directory Services, group names do not need to be unique. By default, RES Workspace Manager Directory Services based on Novell will use the full paths of these groups to distinguish between them. This can be disabled, so that RES Workspace Manager will treat all groups with the same name as one.

For example, you have the Organizational Units "New York" and "Amsterdam", which both contain a group "Helpdesk". Users from both those groups need access to the application "Knowledge Base". The way in which Access Control is set for this application, depends on the option **Use full group names** in the RES Workspace Manager Directory Service for this Novell environment:

- If the option **Use full group names** is selected for the Directory Service for this Novell environment, Access Control on the application "Knowledge Base" must be set on the group Amsterdam/Helpdesk AND on the group New York/Helpdesk.
- If the option **Use full group names** is not selected, Access Control on the Knowledge Base can be set to the group "Helpdesk", and this will automatically include all groups with that name in that Novell Directory Service.

Security Context

Ensure that the **Security Context** fields of the Directory Service are filled out if Citrix XenApp Integration is enabled in your RES Workspace Manager environment.

- Give the full path to the user name, for example: admin1.administrators.newyork.resdemo

Notes

- Per RES Workspace Manager environment only one Novell Directory Service can be configured.
- RES Workspace Manager support for Novell Directory Services requires Netware 4.x or higher. In combination with Citrix, a higher version is required: Citrix 4.0 and 4.5 (x32 and x64) require Novell 6.5; and Citrix XenApp 5.0 supports Novell 6.5 too, but only on Windows 2003, not on Windows 2008.
- If the Novell client has not been installed on the target computer, RES Workspace Manager will use standard Windows NT user and group enumeration for any user who logs on.

5.11 Workspace Branding

At **Workspace Branding** in the **Setup** menu, you can customize the splash screen that is displayed when starting, refreshing and ending an RES Workspace Manager session and when starting the RES Workspace Manager Console. The custom image that is selected is automatically resized to fit the splash screen. This image (same size as used in the splash screen) also replaces the RES Workspace Manager logo in the background of the Management Console.

Configuration

Upload the custom image, select an RGB color for the progress bar and give the new workspace branding style a name. The workspace branding that is selected as active style will be applied in the entire RES Workspace Manager environment and cannot be selected per Workspace Container.

Note

Workspace Branding is available in the **Delegation and Compliance** module (*i.e.* Silver (Administration), Gold and Enterprise license editions).

Chapter 6: Access Control

Access Control determines users' access to RES Workspace Manager settings and applications. Access Control consists of:

- **Identity**: which users get the setting or application. By default, all users are allowed access.
- **Locations and Devices**: in which Zones or on which clients the setting or application is available. By default, access is allowed from all zones and clients.

If none of these areas is configured for an object, the object is available to all users throughout the RES Workspace Manager environment.

If one or more of these areas is configured for an object, users get access if they meet the criteria specified in each configured area.

6.1 Identity

Depending on the item you are setting Access Control to, the following Identity options are available:

- All Users
- User/Group
- NOT User/Group
- Organizational Unit
- Organizational Unit including child OUs
- Controlled by Application Manager(s) (only for applications)
- Administrative Role
- NOT in Administrative Role
- Language
- RES IT Store Service
- Not RES IT Store Service

Note

Not all Access Control options may be available, depending on the item to which the setting applies. For example, if you are configuring Access Control for User Settings, you can only select organizational units, groups, users and Administrative roles.

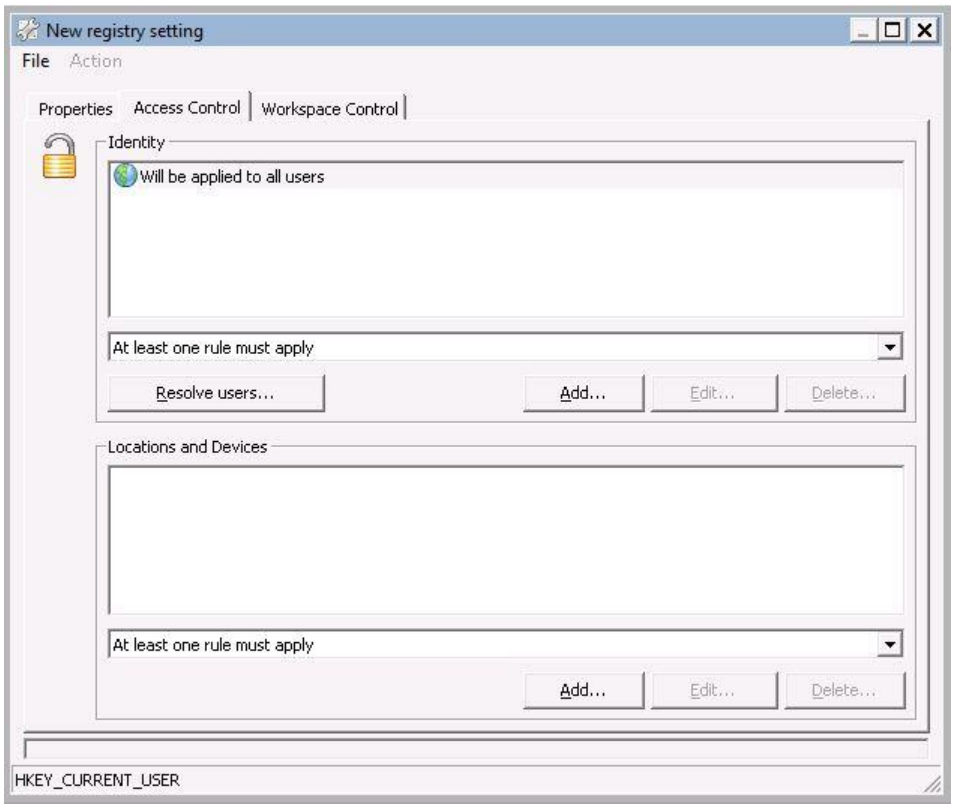
All Users

Select this option if the application or setting should be available to all users in your RES Workspace Manager environment.

(NOT) User / Group

If you use NT-groups to determine access, select the appropriate domain and search for the users/group(s) that need(s) access.

If multiple domains have been configured, you can select several groups from each domain.



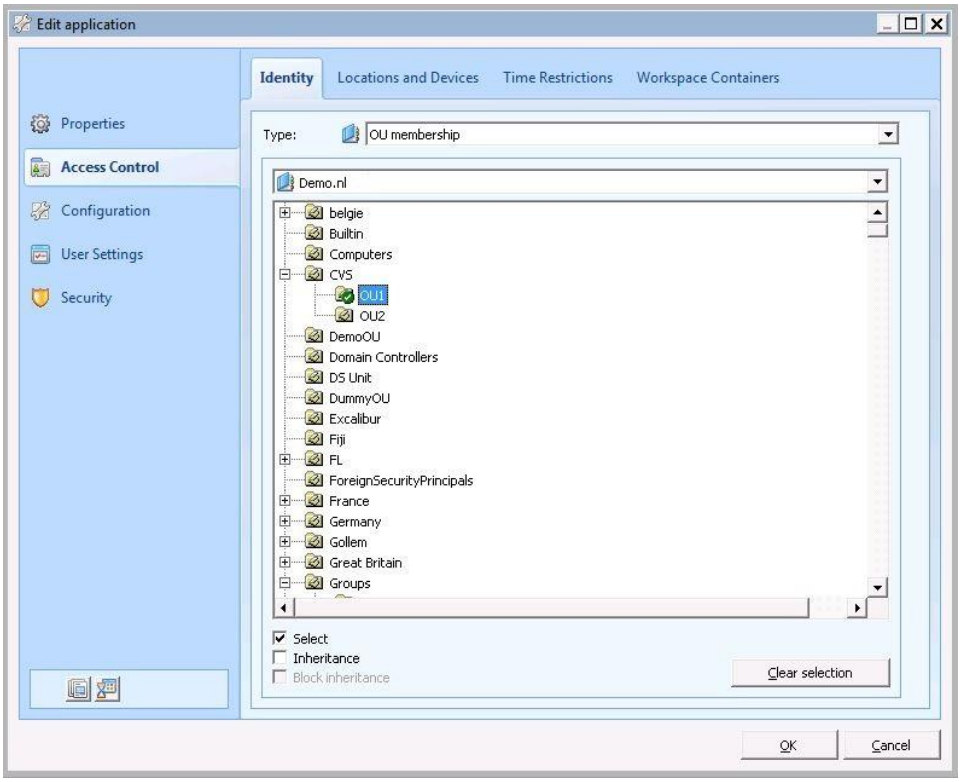
If you are configuring Access Control for an application, you can add groups manually by clicking the button **Add manually**. Specify the name of the group in the popup window and verify it by clicking the **Check** button. You can also use `.\` (dot back slash). This allows you to add a local account once for multiple machines. By default the computer name and user name or group name are shown, for example, `WSL-121\localuser`. By using `.\` it will be shown as .\user name, which makes it applicable to any computer.

You can also add specific users from groups without access: fill in their user names and verify these by clicking the **Check** button.

OU membership

You can grant users access based on Organizational Units within Active Directory Services or through groups in the domain. This enables you to use the company's organizational structure to make applications available to the users.

RES Workspace Manager enables you to use these grouping features in a Windows environment. By selecting the appropriate option, you can grant access to users based on their OU. Remember to select **Inheritance** (when setting Access Control to an application) if relevant.



(Not in) Administrative Role

You can use Administrative roles as access principle when configuring Access Control criteria. You can use the Administrative Role "Technical Manager" as an access principle to grant access to an application to all users to which this Administrative Role applies.

Language

You can also use languages as access principle when configuring Access Control criteria. For example, if the Console contains a French version of Adobe Acrobat, you can use the language **French** as access principle in Access Control, to ensure that only users that selected the language **French** in their "Workspace Preferences" tool get access to this application. See Languages for more information.

(Not in) RES IT Store Service

You can use the RES IT Store Service access principle. For example, you can base Access Control to the managed application Microsoft Visio on the RES IT Store Service "Microsoft Visio". This enables you to use the RES IT Store workflow to approve and install the application, while RES Workspace Manager automatically makes the managed application available as soon as the service is actually delivered in the end user's workspace.

You can select a service from the **Available Services** list or create a **New Service** with the **RES IT Store Service Wizard**. This wizard will guide you through the different steps to create a new RES IT Store service to use in Access Control.

See **RES IT Store** (on page 187) for more information.

6.2 Locations and Devices: Zones

Access to a RES Workspace Manager object can depend on the location where and the device on which a user session is started.

These locations are defined as Zones, based on various criteria such as IP-addresses, computer names, hardware requirements, environment variable values, operating system versions, USB storage device serial numbers, etc.

Zones are selected as Access Control criterion in the **Locations and Devices** area.

6.2.1 Zone rules

- Rules based on **Active Directory Site** allow you to create zones based on the Active Directory site from which users can start a RES Workspace Manager session. This can be useful for sites with multiple Active Directory sites, divided by different domain controllers.
- Rules based on **Active Directory Group membership** allow you to set access on items, based on computer group membership.
- Rules based on **Active Directory OU membership** allow you to set access on items, based on computer OU membership.
- Rules based on **Active Directory User property** are useful to create Zones for applications and/or settings that should only be available in sessions that match the value of the specified user property. For example, when an application should only be available to users in a specific company department, you can create a Zone rule based on the user property "department" and a value that specifies this company department.
- Rules based on **Computer Hardware** are useful for applications that need specific minimum system requirements (for example, AutoCAD).
- Rules based on **Processor architecture** (under **Computer > Hardware**) are useful for applications that need specific processor type (x86/x64).
- Rules based on **IP address, IP address range** or **Computer Name** (under **Computer**, **Network** and **Remote Desktop**) are useful to link the Zone to a range of IP addresses or to a specific server, for example when configuring a printer server. When adding a Rule based on the **Computer name** for a Zone, the **Computer (FQDN)** can be used to apply the Rule to one or several Zones.
- On the **Rules** tab of a zone based on **Computer name**, you can manually add the relevant computer names.
  Specifically for this type of zone, computer names can also be added to an existing zone using the command line. This can be used, for example, for scripting. The Administrator who runs this command must have access to the Console and to Zones.
- Rules based on **Operating system (Bit) version** (under **Computer** and **Configuration**) are useful for applications that need a specific (bit) version of a Microsoft Windows OS.
- Rules based on **Vendor ID, Product ID or Serial number of USB storage devices** (under **Computer** and **Configuration > Hardware token**) allow you to create advanced scenarios in which, for example, an application is only available or a laptop can only be accessed if a specific USB storage device is present. For more information, see **Zone examples - Using a USB device for authentication purposes**.
- Rules based on **Environment variable** (under **Configuration**) allow you to set access on items, based on the value of a specific environment variable. This rule applies to existing environment variables only; not to environment variables that are set by the Workspace Composer when the user starts a session.

- Rules based on **File version** (under **Configuration > Files and folders**) are useful if the version of a specific file should be the reason why a setting or application should be available or unavailable. For example, access to a database can be made to depend on the version of the database client; or the availability of an application can be made to depend on the version of a DLL file. In this way, you can hide an application from a user if the application cannot function properly due to the absence of a required version of a specific file. This saves the user from opening the application and then being confronted with error messages and other problems.
- Rules based on **File or folder exists** (under **Configuration > Files and folders**) are useful if the existence of a specific file, folder or drive at the start of a session should be the reason why an action should be carried out or not. For example, you may want to perform a folder synchronization action with a network drive. This action is only useful if this drive mapping exists. The Zone rule **File or folder exists** can be used to check this.
- Rules based on **Federal Information Processing Standard (FIPS) compliancy** (under **Configuration**) allow you to set access to resources based on a FIPS-compliant Windows Operating System. The rule evaluates whether the Windows GPO for FIPS has been set on the Agent.
- Rules based on **Registry setting** (under **Configuration**) offer a huge range of possibilities, because much information is stored in the Registry. Each piece of information in the Registry can serve to determine the user's workspace, from printers to environment variables to applications to Data Sources. For example, the availability of Word 2007 can be made to depend on a Zone that checks for the Registry key `HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word`; and the availability of Word 2003 can depend on the absence of this key. Similarly, different language versions of an application can be made available to users depending on their Active Directory site, which is stored in the Registry. Or access to the plotter printer can be granted only to users who use an AutoCAD application, as information about this is also stored in the Registry.
- Rules based on **Remote host/URL** (under **Network**) allow you to verify whether a specific IP address or URL is reachable to define an Access Control mechanism. This may be useful, for instance if a specific URL is only available from within the company network. Setting Access Control on an application to a Zone based on Remote host/URL prevents the application to be started from another location.
- Rules based on **Connected network (SSID)**, allow you to configure features (e.g. printers) that are available if a session is running on a device connected to a specific wireless network.
  - Rules based on the **Security** option **Must connect through a trusted access point** apply if the Agent's connection to a wireless network with the specified SSID uses a trusted access point. This makes it possible to disregard connections to other wireless networks with the same SSID, because they will not be accessible through your trusted access points.

    Please note, an access point is trusted if an enabled **Nearest access point (BSSID)** zone rule exists for it in your RES Workspace Manager Console. Please be sure to define a full set of relevant access points.
  - Rules based on the **Security** option **May connect through any access point** apply if the Agent is connected to any wireless network with the specified SSID. This may or may not be your organization's wireless network, because wireless network SSIDs are not globally unique.

    This option may be sufficient if you have not defined a full set of trusted access points, and/or if security is less important.
- Rules based on **Nearest access point (BSSID)**, allow you to configure features to be available if a session detects that a specific access point is the nearest, based on it having the greatest signal strength of all detected access points.
  Please note that each access point for which a zone rule is specified will become a trusted access point for the purpose of zone rules based on wireless networks.

- Rules based on the **Signal detection** option **Limit to trusted access points** will only evaluate trusted access points when determining which detected access point has the greatest signal strength.

  Please note, an access point is trusted if an enabled **Nearest access point (BSSID)** zone rule exists for it in your RES Workspace Manager Console. Please be sure to define a full set of relevant access points.

- Rules based on the **Signal detection** option **Do not limit to trusted access points** will evaluate all detected access points from networks with the specified SSID when determining which detected access point is the nearest. Detected access points may include mobile access points to other networks with the same SSID, because wireless network SSIDs are not globally unique.

  This option may be sufficient if you have not defined a full set of trusted access points, and/or if security is less important.

- Rules based on **Client type (Citrix Receiver only)** (under **Remote Desktop**) allow you to create zones based on the client type detected through the Citrix Receiver on Citrix XenApp and Citrix XenDesktop. This leverages the support that Citrix Receiver provides for different devices in order to distinguish the various operating systems.
- Rules based on **Session type** (under **Remote Desktop**) allow you, for instance to easily distinguish various desktop types. By specifying a session type, protocol and/or platform, access to a Zone may be set accordingly. A zone specifically for XenDesktop machines, for instance, would comply to: Session type: Remote Desktop; Protocol: Citrix ICA; Platform: Desktop. Other supported protocols are: Microsoft RDP, VMware PCoIP and VMware Blast.
- Rules based on **Terminal Server (TS) listener name** (under **Remote Desktop**) allow you to create Zones that can differentiate between network connections from inside and outside the company network. This is useful for applications that should be highly secured, such as financial applications.
- Rules based on the presence (or absence) of a **VDX/Workspace Extender** (under **Remote Desktop**) are useful to create Zones for applications that should only be available when there is (or is no) active VDX or Workspace Extender Client. These rules also apply to the RES Subscriber for VDX Agent and RES Subscriber for VDX Client.

Notes

- It is also possible to add a rule based on a computer name to an existing Zone, using a command line. In the RES Workspace Manager Console this would be done at **User Context > Locations and Devices**, **New/Edit Zone** and then selecting the **Rules** tab and adding a **Computer Name**. This option is also available in combination with the command line, which can be used, for example, for scripting. Some examples of the syntax that can be used:
  - to add MACHINE002 to the zone "France > Paris > Building A > Floor 1", the following command line can be used:

    ```
    pwrtech.exe /clientadd=MACHINE002 /zone={7B8BF240-3682-41C5-881E-B14595593817}
    ```

  - if the command is run without a value for the parameter `/clientadd`, the current computer on which the command is run will be added:

    ```
    pwrtech.exe /clientadd /zone={7B8BF240-3682-41C5-881E-B14595593817}
    ```

  - if the command is run with a question mark as the value for the parameter `/zone`, a selection window is opened allowing the administrator to select the Zone:

    ```
    pwrtech.exe /clientadd /zone=?
    ```

  - to remove a Zone Rule for a particular client from a particular Zone:

    ```
    pwrtech.exe /clientremove=MACHINE002 /zone={7B8BF240-3682-41C5-881E-B14595593817}
    ```

  - if the command is run with an asterisk (*) for the parameter `/zone`, all existing Zones are checked and any Rule where the (partial) computer name = MACHINE002 will be removed:

    ```
    pwrtech.exe /clientremove /zone=*
    ```

- **Active Directory Group membership** is supported for:
  - Active Directory groups
  - NT Domain groups
- If an access point is configured to hide its SSID, RES Workspace Manager will detect it as an empty SSID (i.e. empty string). If there are multiple access points with a hidden SSID, RES Workspace Manager is not able to distinguish between the networks they belong to. In this case, a rule for the nearest access point, specified for an access point with a hidden SSID, will check the nearest access point of ALL access points that hide their SSID (even if they belong to different networks).
- The use of environment variables is not supported for SSID and BSSID names.
- Due to privacy constraints, detected wireless networks and access points are not logged in the RES Workspace Manager Console. However, during a user session they are shown to the end user on the **Diagnostics** tab of the Workspace Preferences tool, so end users can provide their administrator with this information upon request.

6.2.2 Multiple Rules for a Zone

By default, a Zone applies if a user logs on from a computer that matches *one* of the specified rules.

By grouping Zone rules using the **ampersand** button  , you can divide rules into groups. The ampersand functions as a group separator, and the Zone applies when one of the groups of rules is met.

Examples

Item	Explanation
Zone A Rule 1 Rule 2	Accessible when Rule 1 OR Rule 2 applies (or both).
Zone B Rule 1 & Rule 2	Accessible when Rule 1 AND Rule 2 apply.
Zone C Rule 1 Rule 2 & Rule 3	Accessible when Rule 1 OR Rule 2 applies (or both), AND Rule 3 applies.
Zone D Rule 1 Rule 2 & Rule 3 Rule 4	Accessible when Rule 1 OR Rule 2 applies (or both), AND Rule 3 OR Rule 4 applies (or both).

When adding Zones in **Access Control** / **Locations and devices**, it is possible to require all Zones to be valid by using the AND option. For example, if you have a Zone for a particular OS and another Zone for a particular hardware requirement, you can combine these two by using AND in one Zone Rule. This way you do not have to create a third Zone to combine the two Rules.

6.2.3 Zone Members: Nested Zones

A Zone can be a member of another Zone. This allows you to arrange Zones in a parent/child hierarchy.

If a Zone contains no rules but only members, the Zone applies if the user logs on at a computer for which **at least one** of the member Zones is accessible.

If a Zone contains rules as well as members, the Zone applies if the user logs on at a computer for which all the Zone rules are met.

If a Zone contains rules and it also has a parent Zone, then the Zone applies if the Zone rules are met.

Example

- Zone A (no rules, only member Zone)
- Zone B (no rules, only member Zones)
- Zone C (contains rules)
- Zone D (contains rules)

In this example:

- Zone A can be accessed if Zone B can be accessed.
- Zone C can only be accessed if the rules of Zone C are met.
- Zone D can only be accessed if the rules of Zone D are met.

6.2.4 Pattern matching in Zones

Pattern matching allows you to use wild card characters, character lists and character ranges in any combination to match a certain value (for example, client names or IP addresses). The specified pattern is used to find the desired data. If necessary, you can test a certain pattern before you use it in a field.

You can use the following pattern matching characters when configuring Zones:

Character	Explanation
`?`	Any single character
`*`	Zero or more characters
`#`	Any single digit (0-9)
`[Charlist]`	Any single character in charlist
`[!Charlist]`	Any single character not in charlist

6.2.5 Example: Using a USB device for authentication purposes

By restricting an application or setting to a Locations and Devices Zone based on the unique serial number of a USB storage device, you can turn this specific USB storage device into a key to the application or setting.

Procedure

1. At **User Context > Locations and Devices**, create a Zone based on the rule **USB storage device > Serial number**.
2. At **Advanced Settings** in the **Setup** menu, select **Refresh Workspace on USB storage device change**.
3. Set the Access Control of the application or setting to require the Zone.

With this setup, the user's session is refreshed when a USB storage device is plugged in. If the serial number of the USB storage device matches the Zone rule, the application or setting becomes available. When the USB storage device is unplugged, the session refreshes again and the application or setting is no longer available.

This setup also works if the session is a Workspace Extension using the Workspace Extender.

6.3 Connection States

Use the **Connection States** node of the **User Context** section to configure the connection state settings of computers in your RES Workspace Manager environment. This allows you to specify which applications and/or settings that are configured for off- and online use will be available to the user.

There are two different methods of detection of the connection state in RES Workspace Manager:

Default detection of Connection State: if the connection state of the computer is required for a setting or for accessibility to an application, the IP-address of the local network connection will be used for this task. If no IP-address is available, an "offline" Connection State will be assumed.

Advanced detection of Connection State: in certain conditions, the default method to detect the Connection State will fail. For example, if a fixed IP-address is assigned to the local network connection, the detected Connection State will always be "online". By using "Advanced detection", this problem can be solved. Computers with access to any listed Zone will only have an "online" Connection State if the specified IP-address can be detected.

It is also possible to select detection based on hostname, port and URL (http/https). By specifying an IP Address, an IP Address and a port, or an URL (http/https), you can verify whether a specific IP Address or URL is reachable to define an online or offline Connection State. This may be useful, for instance if a specific URL is only available from within the company network. Setting the advanced connection state to detect this URL allows you to use **Advanced detection of Connection state** to determine whether a laptop is used inside or outside the company network. This might especially be useful to, for example, prevent company-sensitive information to be available outside the company.

6.4 Languages

Use the **Languages** node of the **User Context** section to extend multilingual support in your RES Workspace Manager environment. Multilingual support in RES Workspace Manager is primarily based on LanguagePacks. LanguagePacks provide different languages for all RES Workspace Manager components, which end users can select in their "Workspace Preferences" tool.

By mapping languages to a LanguagePack, you can present the end user with a choice of additional languages to those available in LanguagePacks. This allows you to configure environment variables or registry settings that can be used to base applications on the language selection of the end user.

To map a language to a LanguagePack select **Enable mapping of language to LanguagePack**. This will display a list of available languages. Select a LanguagePack in the Installed LanguagePacks area and select the language(s) that you want to map to this LanguagePack.

Example:

If you highlight LanguagePack **English** and select the language **Norwegian (Nynorsk)**, the variable `%LCID%` will contain the Windows identifier of that language. You can then use this variable to make changes in the registry on language level. For example, if you change the registry using this variable, you can change the display language of Microsoft Office.

After you have mapped Norwegian (Nynorsk), the user can select Norwegian (Nynorsk) in his "Workspace Preferences" tool. After refreshing the Workspace Composer, RES Workspace Manager will display an English interface, whereas Microsoft Office will display the Norwegian (Nynorsk) interface.

Access Principle

You can also use languages as access principle when configuring Access Control criteria for a certain setting or application in RES Workspace Manager. For example, if the Console contains a French version of Adobe Acrobat, you can use the language **French** as access principle in Access Control, to ensure that only users that selected the language **French** in their "Workspace Preferences" tool get access to this application.

6.5 Application Delegation

An option for granting users access to an application is to delegate this task to other users or Groups. Specific people who are expert users or who are responsible for a certain application can be made **Application Managers**. In most cases these people are non-IT personnel. Application Managers gain access to the **Access Wizard**, an application that allows them to make the application(s) for which they are responsible available to other users.

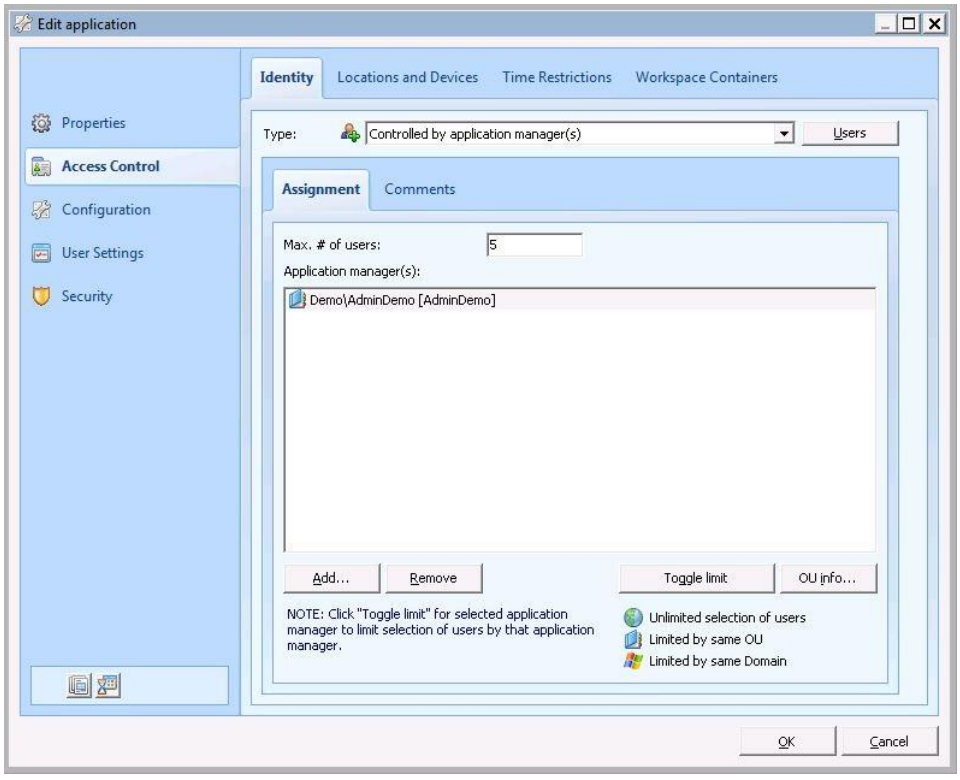
You can assign an Application Manager by first selecting the appropriate Domain (if applicable), and then searching for the Users / Groups you want to make an Application manager.

If you want to see which OU a user belongs to, click **OU info**.

You can toggle the range within which an Application Manager can grant access to the application: select the Application Manager's name and click the button **Toggle Limit** to limit the application manager's range to:

- all users.
- only users in the same OU as the Application Manager.
- only users in the same domain as the Application Manager.

On the **Comments** tab you can create a message to be displayed by the Access Wizard when an Application Manager grants or revokes application access.



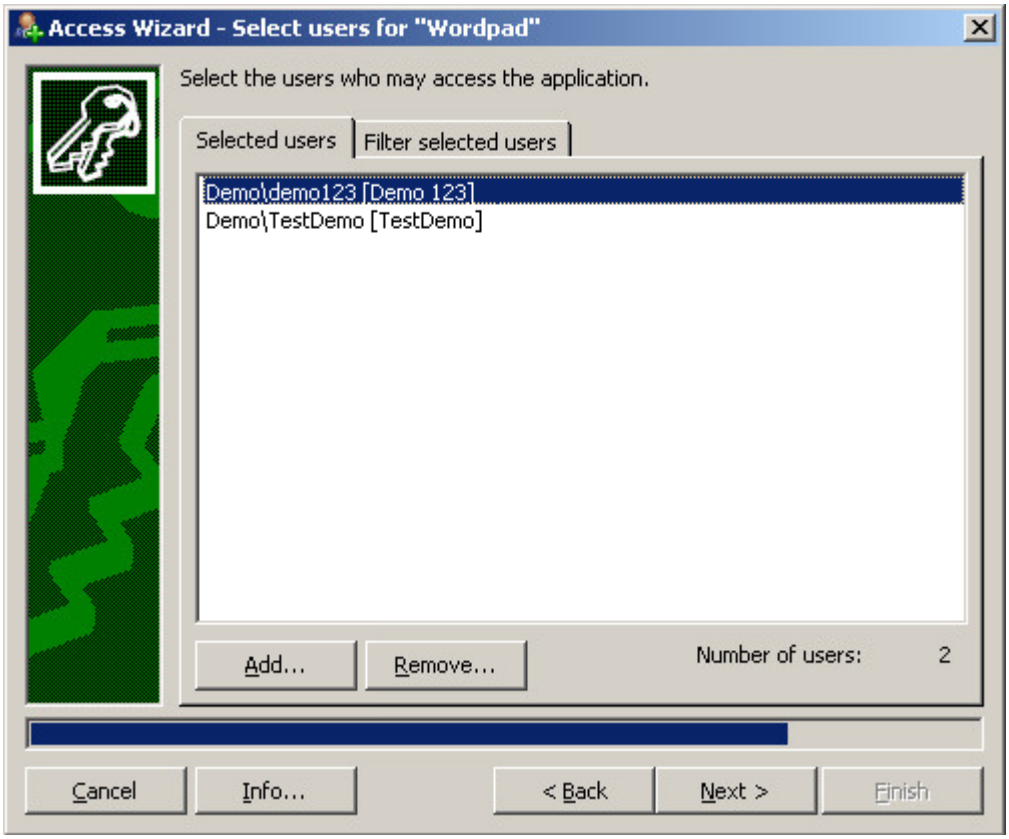
With the Access Wizard the Application Manager can grant or revoke application access in three steps. The Access Wizard can be found in the **Settings** section of the Application Manager's Start menu. When the Access Wizard is started, a dialog box will be displayed with three options:

- **Grant access**
- **Revoke access**
- **View info**

Selecting **Grant access** guides the Application Manager through the process of assigning access. The Application Manager can select an application first and then assign users to it, or he can select a user first and then grant him access to one or more applications.

Selecting a user first and then granting him access can be used when assigning several applications to this user in one action. For example, when a new employee enters the company, he probably needs access to specific applications, based on job type and the department he works at. By granting access based on a user, the Application Manager can perform this action in one session. The users that are visible to the Application Manager may be filtered on OU or NT groups.

By selecting an application first, the Application Manager can assign one application to several users. This is useful when a new application has been installed and an entire department needs to use it.



6.6 Administrative Roles

Use the **Administrative Roles** node of the **Administration** section to manage access to the Console. By assigning an Administrative Role to an administrator of RES Workspace Manager, you can define his access permissions and scope of the Console and thereby define what he is allowed to manage.

Each Administrative Role is defined by the following aspects:

- its **permissions** determine which nodes and objects are shown in the RES Workspace Manager Console, and whether they can be viewed or edited.
- its **Scope Control** determines the users and Workspace Containers for whom the Administrative Role can edit objects in the RES Workspace Manager Console. This is based on the Access Control and Workspace Control set on those objects. See **Scope Control** (on page 69).
- the **Access Control** and **Workspace Control** set on the Administrative Role determine which users get the Administrative Role in which locations and Workspace Containers. See **Workspace Containers** (on page 235).

Administrative Roles

Users, groups, and OUs, and Zones can be assigned to **read** or **modify** specific nodes of the Console by creating Administrative Roles.

To create an Administrative Role:

- Click **Add** to create an Administrative Role.

Click the **Settings** tab to assign the security permissions of the Administrative Role.

- Enter the name of the Administrative Role in the **Name** field.
- Click the appropriate nodes to assign **Deny** access, **Read** and **Modify** permissions. By default, all nodes will be assigned **Deny** access permissions. You can grant different levels of access to a feature's settings and to its list of rules or objects. For example, at **Composition > Printers** you can assign **Modify** permissions to a Console user for the **Printers** tab, while assigning **Read** permissions to the **Settings** tab and any exception tabs of the **Printers** node.

Optionally click the **Scope Control** tab to configure the scope of the Administrative Role. See **Scope Control** (on page 69).

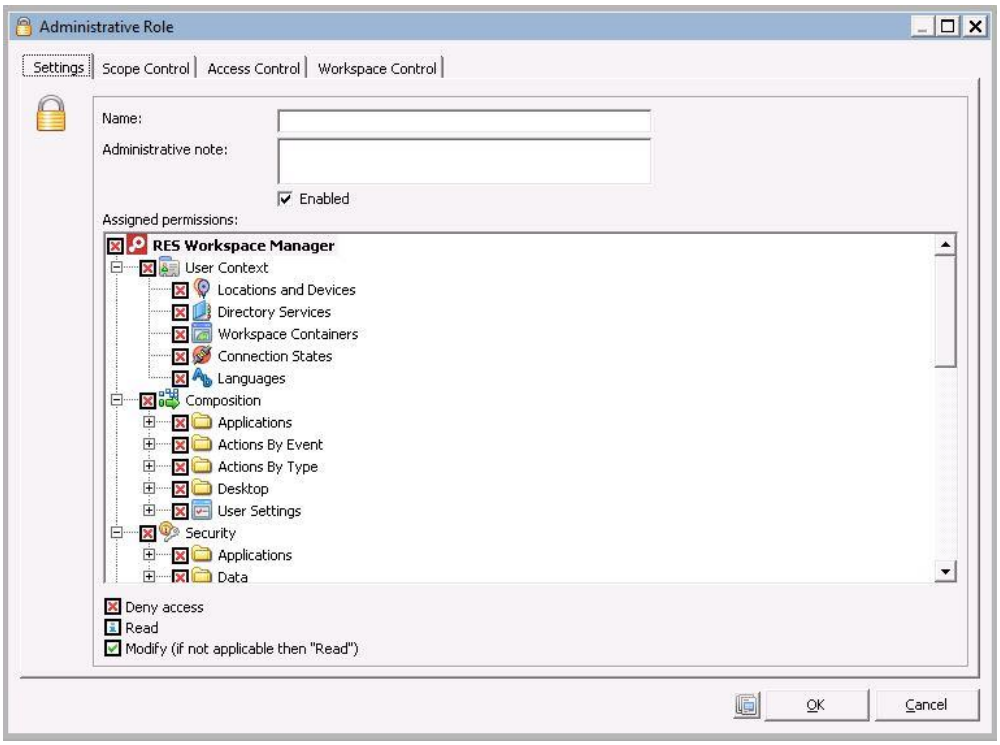
- Click the **Access Control** tab to select to which administrators the **scope** applies.
- In the **Identity** area, click **Add**. This will open the Identity window.
- Click **Resolve users** to retrieve information about the users that you assigned. This will open the **Assigned users** window.
- Click the **Workspace Control** tab to configure to which Workspace Container(s) the **scope** applies.

Click the **Access Control** tab to configure to which administrators the **Administrative Role** applies.

- In the **Identity** area, click **Add** to select groups and/or users. This will open the **Identity** window.
- Click **Resolve users** to retrieve information about the users that you assigned. This will open the **Assigned users** window.
- In the **Locations and Devices** area, click **Add** to select a (NOT in) Zone or Client name.
- Alternatively, click **Edit** or **Delete** to change existing entries.

Optionally click the **Workspace Control** tab to configure to which Workspace Container(s) the Administrative Role applies.

- Select the applicable Workspace Container(s).
- Click **OK** to close the **Administrative Role** window.



The Administrative Role **Technical Manager** can never be removed, disabled, renamed, or assigned to different permissions. It is also mandatory to assign at least one user, group, or Organizational Unit to the "Technical Manager" role. When performing an installation of RES Workspace Manager, the Administrative Role Technical Manager will be created automatically.

Administrative Roles can be added, edited, deleted, or duplicated. If a new Administrative Role is added, permissions can be assigned to each node of the Console (**Deny access**, **Read**, and **Modify**). By default all nodes have **Deny access** permissions. Access control to the Administrative Role is added based on groups, users, or Organizational Units. If Zones are assigned, the Administrative Role is only accessible from those locations. If no Zone is assigned, the Administrative Role is not limited by location.

If you are able to access the Console, one or more Administrative Roles are assigned to you. All assigned Administrative Roles will be applied, even if more than one is assigned. Multiple permissions for the same node are applied in this order: **Deny**, **Read**, **Modify** (**Modify** takes precedence over **Read**, and **Read** takes precedence over **Deny**).

To find out what Administrative Roles are assigned to you, click **Options** in the menu bar of the Console and select **Show My Administrative Role(s)**.

To resolve all users assigned to a specific Administrative Role, edit the Administrative Role, select the **Access Control** tab and click the **Resolve users** button. Users are listed based on assigned users, groups (group nesting may apply), and Organizational Units.

Workspace Analysis presents a complete overview of users and their assigned Administrative Roles. See **Workspace Analysis** (on page 241). If you view the Workspace Analysis details of a user, the assigned Administrative Roles are listed under **User Context > Account properties**.

Notes

- In RES Workspace Manager 2012, the tabs of many features have been split in an objects tab and a **Settings** tab. When upgrading to RES Workspace Manager 2012 or higher, the permission that was assigned to the **Properties** tab in RES Workspace Manager 2011 will be copied to both tabs after the upgrade. For example, if an Administrative Role had read-only access to the node **Composition > Printers**, that Administrative Role will have read access on the tabs **Printers** and **Settings** after the upgrade.
- If RES Workspace Manager 2012 or higher is downgraded to an earlier version, the lowest of the permissions set on the two tabs will be applied. For example, if an Administrative Role has modify rights to the **Printers** tab and read-only access to the **Settings** tab, the Administrative Role will have read-only access to the node **Composition > Printers** after the downgrade.

6.6.1 Scope Control

Administrative Roles determine which objects a user of the RES Workspace Manager Console is allowed to see and to manage. This enables delegation of control over the RES Workspace Manager site.

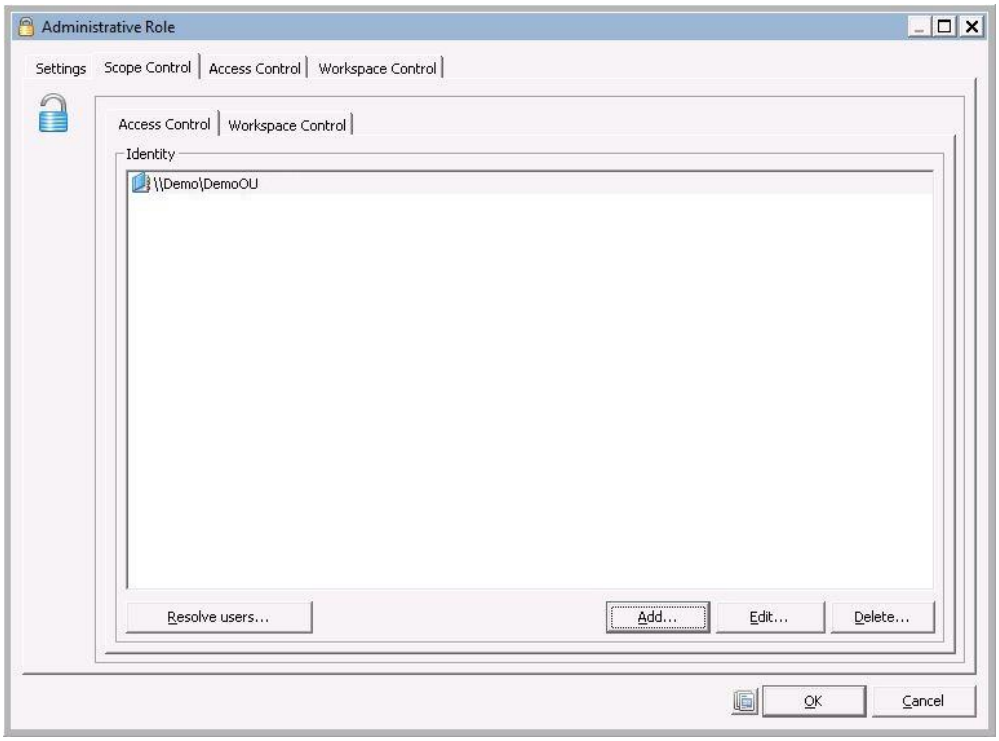
Define **Scope Control** to determine which applications and settings in the RES Workspace Manager Console can be **viewed** or **changed** by the Administrative Role, based on the **Access Control** and **Workspace Control** of these objects.

With the Scope Control Access Control set to a specific Organizational Unit, for example, the administrator can only modify applications and settings that are assigned to users in that Organizational Unit. Applications and settings that are assigned to users in a different Organizational Unit, or that also have additional different Access Control criteria, cannot be modified.

This makes it possible to give an administrator in a regional office control over the applications assigned to users from that office, but not over applications that are also used in other parts of the RES Workspace Manager site.

- Global settings for which no Access Control applies, such as Shell exceptions, are always shown, irrespective of the scope of an Administrative Role.
- If an object is not exclusive to the scope of the Administrative Role, it is shown as read-only.
- If an administrator has several Administrative Roles with different scopes, the scopes are added up.
- If an administrator has several Administrative Roles with and without Scope Control, the scoped role overrides the role without a scope.

- When a scope is set to a specific Workspace Container, only Workspace Model exceptions are visible that apply to that Workspace Container. It is not possible to add or edit any exception data, even if they are within that scope.



6.7 Filters

Filters in the RES Workspace Manager Console

Use a filter to restrict the number of objects that are shown in the Management Console, so that you can focus on a specific aspect of your site. This is especially useful in sites that contain a very large number of settings and applications. For example, if you use a filter that is based on a specific Organizational Unit, the Management Console will only show objects for which Access Control is based on this Organizational Unit.

Filtering affects all nodes of the Management Console, except the nodes **Composition > Desktop > Shell** and **Security > Applications > User Installed Applications**. All objects in these two nodes will remain visible in the Management Console, regardless of the filter that is applied. Other Management Console nodes will appear empty if they do not contain objects that match the criteria of the filter that is applied.

Filter types

There are two types of filter:

- A **default filter** shows all the objects for which at least one of the specified criteria applies either *directly* or *indirectly*.
- An **exclusive filter** shows all the objects to which at least one of the criteria applies *directly*.

Examples of the difference between these two filter types

Suppose you want to configure a filter based on the Access Control criterion Organizational Unit (OU) London. The Management Console contains four applications:

- Calculator, with Access Control set to membership of OU London (which is part of OU Great Britain).
- Notepad, with Access Control set to membership of OU Great Britain (with inheritance).
- Wordpad, with Access Control set to membership of Group Trafalgar Square (part of OU London).
- Paint, with Access Control set to "All users".

This results in:

Object	Filtering	Exclusive Filtering
Calculator (Access Control = OU London)	Result: Calculator is shown in filtered Management Console. Reason: Direct relationship.	Result: Calculator is shown in filtered Management Console. Reason: Direct relationship.
Notepad (Access Control = OU Great Britain)	Result: Notepad is not shown in filtered Management Console. Reason: Indirect relationship, but OU Great Britain is parent OU of OU London (higher in the hierarchy).	Result: Notepad is hidden in filtered Management Console. Reason: No direct relationship.
Wordpad (Access Control = Trafalgar Square)	Result: Wordpad is shown in filtered Management Console. Reason: Indirect relationship, because Group Trafalgar Square is part of OU London (lower in the hierarchy)	Result: Wordpad is hidden in filtered Management Console. Reason: No direct relationship.
Paint (Access Control = All users)	Result: Paint is shown in filtered Management Console. Reason: Indirect relationship, because "All users" also includes users who are members of OU London (lower in hierarchy).	Result: Paint is hidden in filtered Management Console. Reason: No direct relationship.

Notes

- If the option Exclusive filter is not selected for a filter, items that would be affected if the option was checked are marked with an "i" (informational) in their icons.
- When filtering on Organizational Unit (OU), nested groups or users across boundaries are not taken into account.

Filter criteria

There are three types of filter criteria:

- Base a filter on **Access Control** criteria to see only objects to which specific users, groups, Organizational Units and/or Zones have access. For example, see all the objects that apply to users in the Organizational Unit "Netherlands".
- Base a filter on **Access Type** criteria to see only objects for which access depends on a specific access method. For example, see all the objects for which access is set according to administrative role (regardless of *which* administrative role), or see all the objects for which access is set depending on Language (regardless of *which* Language).
- Base a filter on **Workspace Control** to see only objects for which access depends on specific Workspace Containers. For example, see all the objects that are available to computers in the Workspace Container "Terminal Servers".

Configuration

- To configure a filter, go to **Action** in the menu bar and click **Configure Filter**.
- You can set several criteria for each type of filter. A filter with multiple criteria shows object that match *one or more* of the filter criteria. For example, if you create a filter based on Access Control with the criteria OU="Netherlands" and OU="UK", then the filter will show all objects for The Netherlands and all objects for the UK.
  - The exception to this rule is an *exclusive* filter on Zones: only objects with a direct relationship with *each* of the Zones will be shown.
- Zone nesting is not reflected in filtering. If Zone A includes Zone B as its member, filtering on Zone A will not show objects that relate to Zone B. To show also objects that relate to Zone B, you also need to add Zone B to the filter criteria. This view will also include objects that only relate to one of these two Zones.

- To reset your filter configuration and restore all defaults, click **Clear filters**. This will return the Management Console to its unfiltered view.
- When you click **OK** after configuring a filter, the filter is applied automatically.

The last configured filter can be applied and disabled by going to **Action** in the menu bar and clicking **Apply Filter**.

Warning

Avoid filters that combine Access Control, Access Type and/or Workspace Control criteria, as the results are difficult to predict.

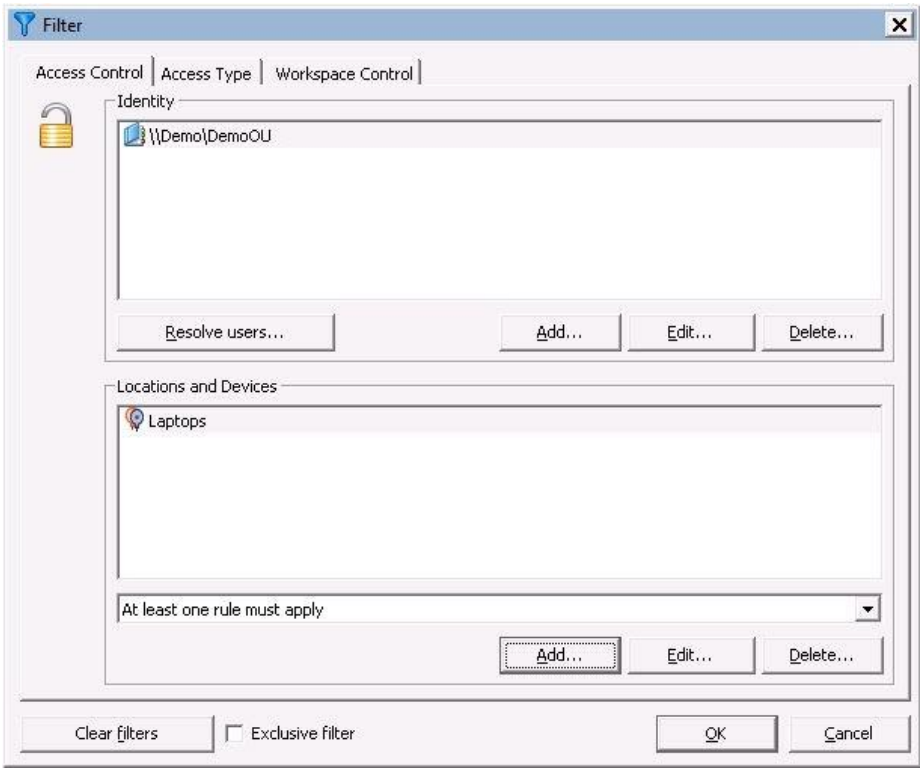
Note

Contrary to the general rule, an *exclusive* filter based on multiple Zones only shows objects that have a direct relationship with *each* of the specified Zones. If the object does not match *all* Zone criteria, it will not be shown in the filtered Management Console. This is different from exclusive filtering based on other criteria, where an object is shown if it has a direct relationship with *at least one* of the specified criteria.

Tip

The Filter Icon in the Management Console status bar shows whether the current view of the Management Console is filtered or not:

- means a filter is active, so you may not see all existing objects in the Management Console.
- indicates that no filter is active, you have a full view of everything in the Management Console.



Chapter 7: Composition

RES Workspace Manager 2014

Now that we have globally defined the user's context, it's time to configure the composition of the user's workspace.

7.1 The End-User Workspace

First of all we will have a look at the end-user workspace itself. End users will encounter the following items:

The Workspace Composer (the actual end-user workspace).

Workspace Preferences (where users can change their personal settings).

Printing Preferences (the users' printer management environment).

PowerHelp (the application information source for users).

7.1.1 The Workspace Composer

The Workspace Composer is the desktop component of RES Workspace Manager.

In a full desktop situation, it is the environment the user works with when using RES Workspace Manager. The desktop provides the functionality that the user needs. This includes all applications, menu items and settings the user is granted access to. It provides the user with a single uniform workspace, regardless of the technology stack used.

The desktop can be displayed with either the **RES Workspace Manager shell** or the **Microsoft Windows shell**.

The RES Workspace Manager shell is a classic windows-like shell with some additional RES Workspace Manager-only technology. The Microsoft Windows shell is the exact shell as it is presented by Microsoft, including the various available themes.

A few of the benefits of the RES Workspace Manager shell are:

- The possibility of displaying additional information in the Taskbar when selecting an application.
- One uniform workspace regardless of the Windows version or technology stack used, which enables smooth OS migrations.
- One company look and feel.

Components of the Workspace Composer

Several icons will be shown in the right corner of the Taskbar, regardless of the shell applied. Each icon has its own specific function.

The user's QuickLaunch icons and the Desktop icon are displayed in the left corner of the Taskbar.

The Desktop icon

Clicking this icon minimizes all running applications at once to clear the desktop.

The Lock icon

This icon invokes the screensaver at any moment. When running RES Workspace Manager on a network-connected desktop or in a Terminal Server session, password authentication for the screensaver is determined by the network setup. It is possible to hide this button at **Composition > Desktop > Lockdown and Behavior**.

If RES Workspace Manager is started by the RES Subscriber for VDX, there are three options for password validation:

- Local
- Session
- None

The Tasklist button

All running applications display their icons in the taskbar, but they can also be displayed by clicking the Tasklist button. This will display a list of all running applications. The user can rapidly switch to another application by selecting it in the task list. It is possible to hide this button at **Composition > Desktop > Lockdown and**

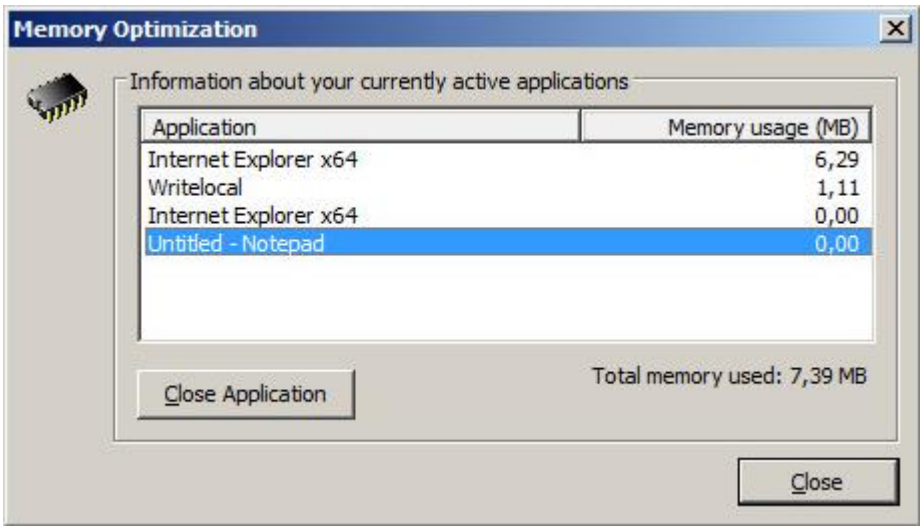
Behavior.

The Memory Optimization icon

The Memory Optimization icon graphically displays the amount of allocated memory currently in use.

Double-clicking the icon will open the **Memory Optimization** window, which displays information about the active applications, their memory usage, the total amount of memory in use and, if applicable, the amount of memory used that exceeds the set limit.

When an application causes the Memory Optimization limit to be exceeded, the Memory Optimization popup window will open. The user can then free up memory by selecting a running application and closing it.



Note

For additional information about Memory Optimization, see Memory Optimization.

Taskbar

The Taskbar provides the user with various additional options:

In the **RES Workspace Manager shell**, the user can display a calendar by double-clicking the clock. Right-clicking the Taskbar enables the user to:

- Access the settings menu and run the "Workspace Preferences" and "Printing Preferences" tools, or the Access Wizard if the user is an Application Manager.
- Run PowerHelp.
- Set Taskbar in tiny mode.
- Log off.
- Refresh the menu.

In the **Windows shell**, right-clicking the Taskbar provides the user with the default Windows options.

Emergency Exit

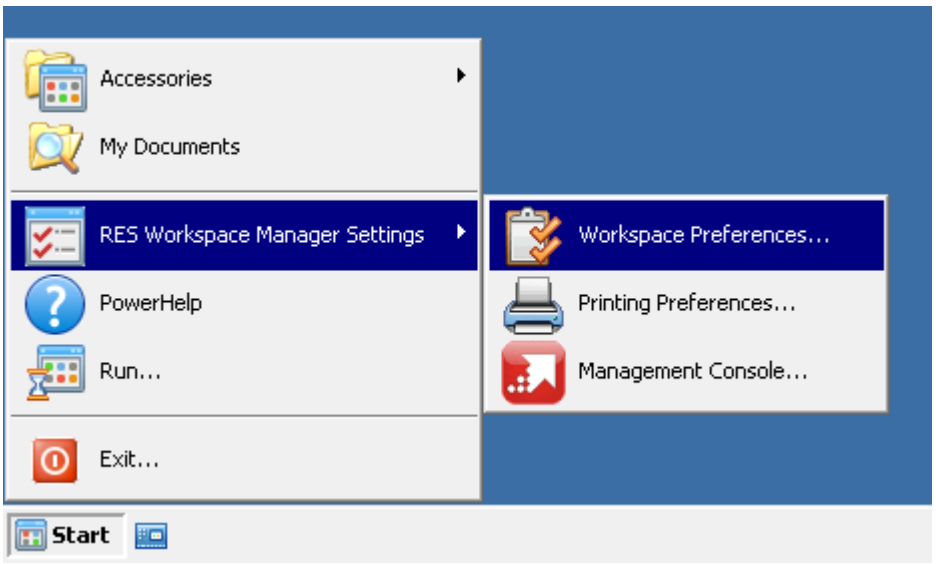
In the RES Workspace Manager shell, an Emergency Exit is available: by double-clicking the upper right corner of the desktop, the user can leave a RES Workspace Manager session immediately. However, if the Emergency exit is used, information about application usage for the session is lost. It is therefore advisable to protect the Emergency Exit with a password. You can do this in the RES Workspace Manager Console (see **Lockdown and Behavior**(on page 139)) by selecting the check box **Protect "Emergency Exit" with password**. The Emergency exit option is never visible on the desktop.

7.1.2 Workspace Preferences

The "Workspace Preferences" tool is the users' desktop management system. It offers users several options, such as configuring their desktop and their taskbar icons, starting applications automatically, or swapping mouse buttons.

When a user has modified his desktop, he can apply the new settings by clicking **Apply new settings now** in his "Workspace Preferences" tool.

The "Workspace Preferences" tool is located in the users' Start Menu in the section **RES Workspace Manager Settings**.



In the RES Workspace Manager Console, you can determine which options should be available in the users' "Workspace Preferences" tool. This allows you to make certain options available or unavailable according, for example, to company policies.

The "Workspace Preferences" tool contains several tabs, each with its own specific use:

- **Start Menu:** applications to be placed in the users start menu.
- **Desktop:** applications to be placed on the desktop.
- **Quicklaunch/Pin to taskbar:** applications to be placed in the Quicklaunch section of the Taskbar or pinned to the Taskbar.
- **Startup:** applications to be started automatically.
- **Background**: change background and foreground colors, and Desktop background picture.
- **Options**: mouse buttons, screensaver, notifications, language settings, and password settings.
- **Diagnostics**: user information.
- **Other**: Usage Tracking, unmanaged applications and Rollback User Settings.

On the **Start menu** tab, users can:

- Determine which application shortcuts should be placed in their Start Menu. By default all available applications are displayed. Users can add or remove applications to and from their Start Menus by disabling the option **Display all available applications in Start menu** and then using the arrow buttons.

On the **Desktop** tab, users can:

- Determine which application shortcuts should be placed on their desktop. Users can add or remove applications to and from their desktops using the arrow buttons.

QuickLaunch/Pin to taskbar, **Pin to Start Menu** and **Startup** tabs

Users can add or remove applications to and from QuickLaunch/Pin to Taskbar, Pin to Start Menu and Startup by using the arrows.

When users select applications on the **QuickLaunch/Pin to taskbar** tab, shortcuts to those applications will be displayed in the desktop Taskbar.

When users select applications on the **Pin to Start Menu** tab, shortcuts to those applications will be displayed in the Start Menu.

When users select applications on the **Startup** tab, these will start up automatically at log on.

When you edit an application in the Console, you can determine whether the application should be available for users to select on the Startup tab.

On the **Background** tab, users can choose their desktop colors. If these colors have been preset according to company policies (in the Console), users will not be able to change these settings.

On the **Options** tab users can:

- Determine after how many minutes their **screensaver** should start. This can also be set by the administrator and is not visible if the screensaver is disabled and no User Setting is set to capture the (unmanaged) screensaver.
- Set the **Taskbar properties**.
- Change their personal **password**.
- Swap the left and right **mouse buttons**.
- Hide the **Description window**, which is normally displayed when users move the mouse pointer over a menu item or application in the menu (in the RES Workspace Manager shell).
- By default the hide printer notification is set to active. If the user has no default printer or if he works remotely on a laptop, the **missing printer** message can be suppressed.
- Disable **Security Management notifications** when an attempt to start an illegal application has been made.
- Select the RES Workspace Manager default **language** at startup. This selection can be linked to the office language set up by the administrator in the Console. When selecting **Default**, all user-specific language settings will be removed.
- With the **Workspace Composer hotkey** users can invoke their Start menu without a mouse. This can be useful when the mouse is not operational and the user has to shut down the computer.
- Icons can be shown in two different **sizes**, large and small. If users use a high resolution, they can use the large icon setting.
- Icons can be **arranged** from top to bottom or from left to right.

On the **Diagnostics** tab the user can:

- Find related technical **information** to communicate with the support department more easily.
- Find information regarding LDAP user entry; Group Membership; Zones, Wireless networks and access points, and Connection State.
- Reload user information (only available if **Do not reload user information when refreshing Workspace** is enabled at **Composition > Desktop > Lockdown and Behavior**)
- Information on the **Diagnostics** tab can be copied. This makes it easier for the user to provide the administrator with Diagnostics information for troubleshooting purposes.

On the **Other** tab the users can see their **Usage Tracking** information (if Usage Tracking is enabled).


On this tab the users can also install, remove or change their access to **User Installed Applications**. This option is only available if has been enabled in the Console.


Restore user Settings. By clicking this button, the end user is able to revert his settings to an earlier stage. This might be useful if the user has made some changes in his settings that he wants to revert, but does not know how, or when he does not exactly know which settings have been changed. For applications, the user is also able to revert to the application's default configuration (if enabled in the Console).

Note

Various options in the "Workspace Preferences" tool can be made (un-)available at the RES Workspace Manager **Composition** section of the **Lockdown** node in the Console. See **Lockdown and Behavior** (on page 139).

7.1.3 Printing Preferences

The Printing Preferences tool is located in the users' Start menu at the **RES Workspace Manager Settings** menu. It provides users with simple printer-related information and a Printer Management console. Only user-related printers are shown. Users can manage their documents and prints by clicking the **Open** button in Printing Preferences.

You can set a default printer by selecting it in the **Available printers** list and clicking the **Set as default** button. If allowed by the RES Workspace Manager administrator, the user may even connect or disconnect a printer if necessary.

In the **Advanced** section of Printing Preferences, additional information is available about the printers and settings related to the user's location. It is possible to select different default printers for different locations. A user's default printer will vary if he works from at home as well as from the office.

To select a default printer for the current location, the user must switch from Basic Printing Preferences to the Advanced Printing Preferences interface. On the left side a list shows the current default printers and locations. On the right side you will find all available printers.

To set a default printer, highlight the printer and select the option **Set as my default printer**. A question will pop up. Click **Yes** if the printer should only be set as default for the current location. Click **No** if it should be the default printer for all locations.

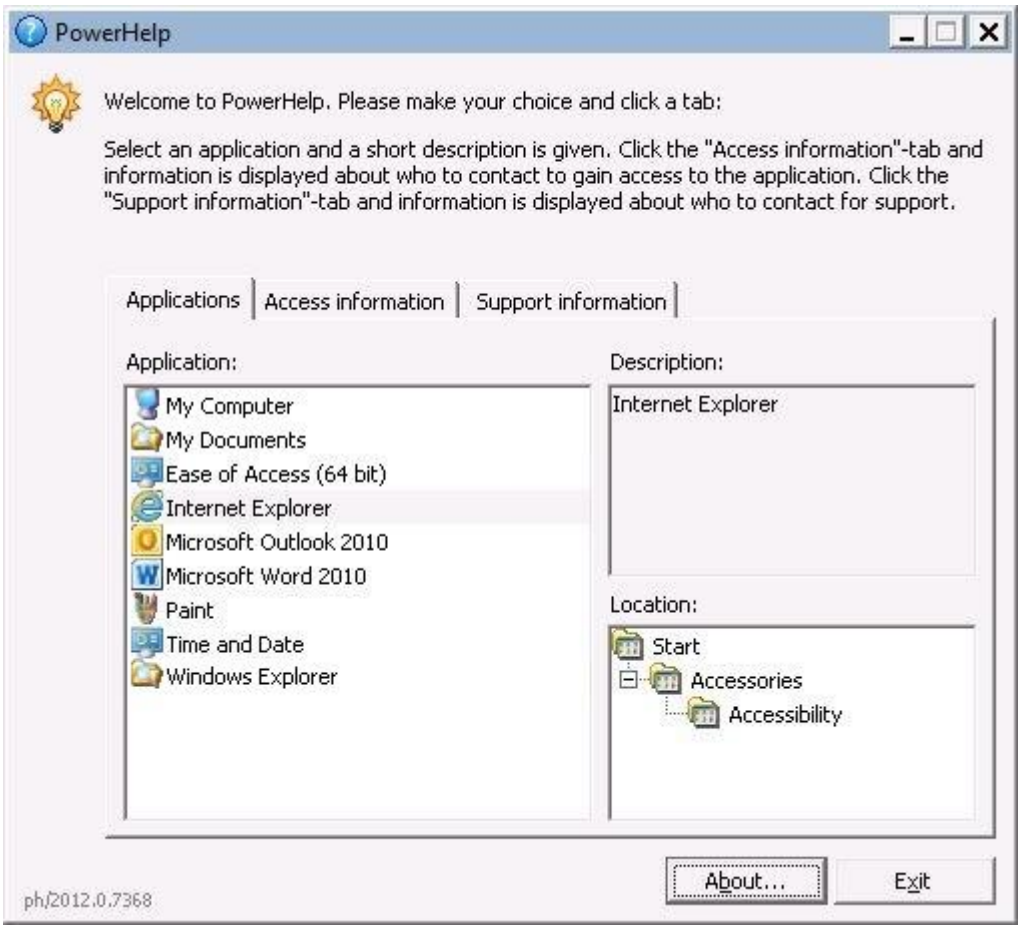
To remove a default printer for a location, select the option **Remove from my default printer list**. If a user switches back to Basic Printing Preferences, all Advanced Printing Preferences are recorded but ignored.

7.1.4 PowerHelp

Next to the Workspace Composer, Workspace Preferences and Printing Preferences, in the end-user workspace, end users will encounter the **PowerHelp**:

In most companies, information about available applications and support is not readily at hand for users. In RES Workspace Manager, **PowerHelp** provides users with information about application availability, application distribution, and application responsibility.

The PowerHelp utility is located in the users' Start menu.



On the **Access information** tab, users can see who the Application Manager of an application is. This can be useful if they have specific questions about an application, or if they need access to it. This provides the company with the possibility to set up a knowledge management organization linked to certain employees (Application Managers) in the organization.

The **Support information** tab provides users with additional information about who to contact for technical support. This is the application manager (if Access Control for the application is set to **Controlled by application manager(s)**) for the application. When no application manager is configured, no additional info will be displayed here.

If **Time Restrictions** apply to the selected application (see **Access Control** (on page 102)), the **Opening times** tab will be displayed. On this tab, users can see on which days and at which hours they are allowed to use the application.

7.2 Desktop Transformation

Desktop Transformation is a concept that transforms an existing desktop infrastructure into managed user workspaces using live data and a step-by-step approach that minimizes the risk and impact on the desktop user.

The transformation process consists of 5 steps:

1. Gather live data from existing desktops.
2. Analyze the data for context.
3. Create workspace items and review impact.
4. Transform existing desktops in small steps with focus on today's challenges first.

Desktop transformation makes use of the following components:

- **The Desktop Sampler** - collects data from unmanaged environments.
- **The Workspace Designer** - designs managed workspace objects based on the collected data.
- **The Workspace Model** - defines which features of RES Workspace Manager should be used.

7.2.1 Introduction to Desktop Transformation

IT departments continuously change the desktop infrastructure as a result of requests for new functionality, cost reduction, and overall quality improvements (integrity, performance). These changes often impact the way an end user works with desktops.

Some examples of changes in the desktop infrastructure are:

- centralization through virtual desktop computing/hosted desktop computing
- upgrade from Microsoft Windows XP to Microsoft Windows 7
- upgrade from Microsoft Office 2003 to Microsoft Office 2010
- implementation of location-based printing
- implementation removable disk security

The first two examples involve comprehensive projects to move end users to a "new" desktop infrastructure. The complexity of these projects makes them difficult to plan and control (time and resources) and impact on the productivity of the end user can be high and unpredictable.

The last two examples are often solved by the use of point solutions. A point solution is a standalone technology for a specific problem that often requires additional management and knowledge. Multiple point solutions are difficult to sustain in the long run. They add complexity and overhead to the desktop infrastructure and IT department.

User Workspaces are a prerequisite for a smooth transition to a new or improved desktop infrastructure. Once User Workspaces are in place, any component of the desktop infrastructure can be replaced with maximum control and without impacting user productivity.

Desktop Transformation provides the answer on how to get from the current desktop state to managed User Workspaces. With this technology, the IT professional is able to transform desktops into managed User Workspaces step-by-step, with a clear understanding of the effects of each action taken. Desktop Transformation is an integral part of RES Workspace Manager.

7.2.2 Desktop Sampler

The **Desktop Sampler** allows the IT administrator to collect information from a desktop. The standalone software can be installed and launched on a desktop. It runs unobtrusively and it collects the following information:

User Context

- User name, logon domain, logon server
- Domain group membership
- Organizational Unit of user
- Computer name, computer domain
- Organizational Unit of computer
- Operating System
- Device Capabilities (CPU/Memory)
- Network IP address

Composition

- Applications exposed in Start Menu
- Drive and Port Mappings
- Network Printers
- Drive Substitutes
- Data Sources

The collected information is stored as a file on a designated file share on the network. One file is created per unique user/computer combination. The IT administrator can configure the Desktop Sampler to uninstall itself after a number of days.

Installing the Desktop Sampler

You need to install the Desktop Sampler on each computer that is to be sampled. This can be a desktop, but also a Terminal Server. The Desktop Sampler installation file `RES-WM-2014-Desktop-Sampler-xxx.msi` is located in the RES Workspace Manager program folder. It consists of a single .MSI file.

Installation

- When you install the Desktop Sampler, it will be installed in the following directory:
  - `%programfiles%\RES Workspace Manager Desktop Sampler` (32-bit)
  - `%programfiles(x86)%\RES Workspace Manager Desktop Sampler (64-bit)`
- Additionally, a `DTSampler` key will be added to the following registry key:
  - `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` (32-bit)
  - `HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run` (64-bit)
- No shortcuts will be added to the user's Start menu.

Command line

You can install the Desktop Sampler by double-clicking the .MSI file or by using a command line. If you use a command line, you can apply the following parameters to the .MSI file:

Parameter	Description
SAMPLEPATH	Specifies the location of the sampled data. This location can also be set in the registry at HKLM\SOFTWARE\RES\Desktop Sampler. If you do not supply a location, the sampled data will be stored in the installation folder of the Desktop Sampler.
EXPIREDAYS=	Specifies the number of days the Desktop Sampler needs to remain installed. After the specified number of days, the Desktop Sampler will uninstall itself. If this parameter is not used, the Desktop Sampler will continue to run until it is manually uninstalled.
DELAY=	Specifies the number in seconds the desktop sampler should wait after a user logs on before it starts sampling data. This is useful when logon procedures take a long time. Specify a number in seconds. By default, the desktop sampler waits for 30 seconds.
NOICONS	Specifies that no icons will be saved to the desktop sampler files.
ALLICONS	Specifies that 256-color and 16-color icons will be saved to the desktop sampler files.
256ICONS	Specifies that only 256-color icons will be saved to the desktop sampler files.

Example: `msiexec.exe /i RES-WM-2014-Desktop-Sampler-xxx.msi SAMPLEPATH=\\fileserver\SampleData EXPIREDAYS=30 DELAY=120 /q`

Command line parameters are case insensitive.

After installation, the Desktop Sampler will sample which applications, printers and data are used by which users at which locations, irrespective of the way in which these settings are managed (manually, scripting, RES Workspace Manager, etc.). It stores this information as a RES Workspace Manager sample file (.DTS). The Workspace Designer uses these files to analyze the sampled information.

All command line parameters can also be used directly when invoking `dtsampler.exe`. For example, after the Desktop Sampler is installed it is also possible to start `dtsampler.exe` with the `/SAMPLEPATH` parameter specifying the path of the generated sample files. This allows the Desktop Sampler also to be distributed as a Custom Resource. This `/SAMPLEPATH` parameter overrules a possible `SAMPLEPATH` parameter used when installing the `.msi`.

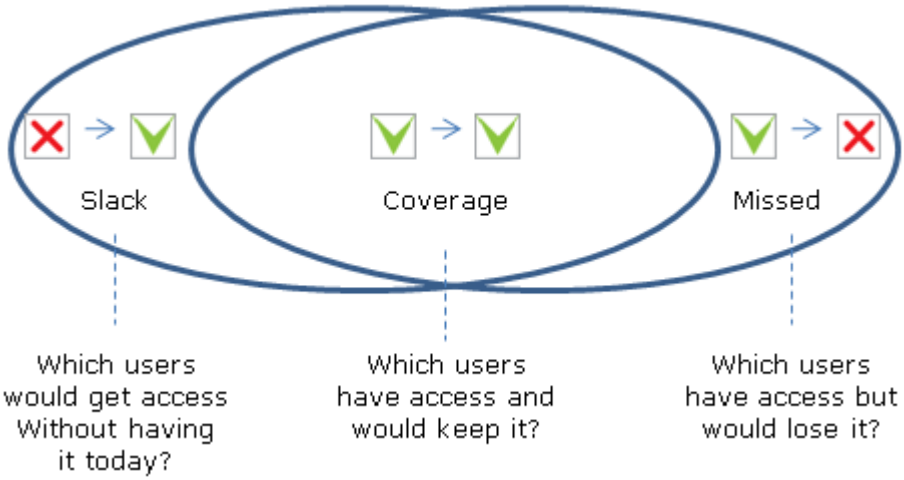
Example:

```
C:\Program Files\RES Workspace Manager Desktop Sampler\dtsampler.exe
/SAMPLEPATH="C:\Temp"
```

7.2.3 Workspace Designer

You can start the Workspace Designer by clicking **Workspace Designer** in the Console. This starts a wizard with which you can analyze the sample files generated by the Desktop Sampler and create and adjust rules based on the sampled data. The Workspace Designer covers the following steps:

- Selection of the type of data to be analyzed (applications, Data Source, Directory Services, Drive & Port Mappings, Drive Substitutes, Locations and Devices, Printers)
- The location of the sample files
- Selection of the objects to be created
- Review of the proposed context rules and their impact, based on:
  - **Coverage**: the percentage of users who currently have the setting, and who will keep it with the suggested rules. (Ideally 100%)
  - **Missed**: the percentage of users who currently have the setting, but who will lose it with the suggested rules. (Ideally 0%)
  - **Slack**: the percentage of users who currently do not have the setting, but who will receive it with the suggested rules. (Ideally 0%)



- Selection and automatic creation of the RES Workspace Manager objects.
- Review of the workspace object, including its **Type** and **Access Control**.

7.2.4 Workspace Model

The Workspace Model shows you the mode in which each feature is running, and allows you to change this if necessary. You can also make this change from the relevant node itself.

It is possible to enable specific parts of RES Workspace Manager, and to disable other parts. This makes it possible to implement RES Workspace Manager gradually, which is very practical if RES Workspace Manager is going to be introduced into an existing environment. Each section of the RES Workspace Manager Management Console has an option to enable or disable it. The settings and configurations of a disabled section are not implemented or executed.

For example, a small number of applications can now be configured in RES Workspace Manager, and merged into the existing Start Menu presented to users. If this goes well, a couple more can be added. In this way, the number of applications managed by RES Workspace Manager can be increased gradually over a period of time, in a controlled manner.

You can change a feature's mode directly from the **Workspace Model**. However, you may prefer to do so from the relevant node itself. There, you can see and amend any related settings, find information about any prerequisites, and access the specific Help about that node (by pressing F1). **Diagnostics** > **Workspace Model Overview** shows you at a glance which features are active/enabled, which are disabled, and which are set in learning mode.

If the global settings of features are overridden by exceptions for specific Workspace Containers, the Workspace Model node shows per Workspace Container which settings apply; either the global settings of a feature or the settings of the exception.

7.2.5 Managed Applications

Managed Applications can be implemented fully, partially or not at all. In a new environment, Managed Applications is disabled: Windows Shell shortcut creation is set to **Do nothing**, so that users get the same Start Menu, Desktop and Quick Launch area in their RES Workspace Manager session as they had outside of the RES Workspace Manager session. With this setup, RES Workspace Manager does not manage any of the user's applications. At this point, you can configure applications in the RES Workspace Manager Management Console, but these are not made available to any users.

If you do not want to manage applications at all, select the option **Disable process interception for unmanaged shortcuts**. This operates on a global level and means that even managed applications that have been configured with interception, will not be intercepted. For a description of the process of intercepting applications, see General at the Properties section of Managed Applications, **If managed shortcut was not used**.

When you are ready to start managing users' applications through RES Workspace Manager, you can enable Managed Applications partially or fully:

- To give users RES Workspace Manager-managed applications in addition to their existing, non-RES Workspace Manager-managed applications, choose Windows Shell shortcut creation: **Merge with unmanaged application shortcuts**. You can combine this option with setting the **Unmanaged shortcuts that point to same executable** option to **Replace with managed shortcut** (at **Properties > Settings** of a Managed Application). With this option you prevent that the user's environment contains both managed and unmanaged shortcuts to the same application.
- To give users only RES Workspace Manager-managed applications, choose Windows Shell shortcut creation: **Replace all unmanaged shortcuts**. This replaces the Start Menu of your users with the Start Menu and application shortcuts as configured in RES Workspace Manager. Unmanaged applications are no longer available.

7.3 Application Management

An important part of creating a RES Workspace Manager environment is creating a menu structure with applications with all the correct settings.

7.3.1 Applications

On the **Application List** tab, the RES Workspace Manager-managed applications that you can make available to users in their Start Menu, Desktop and Quick Launch area are listed.

7.3.2 Start Menu Tab

The **Start Menu** tab shows the applications in the folder structure in which they will appear in the Start Menu. Applications and Start Menu folders are added, edited, disabled and imported from this tab, and existing Windows shortcuts imported. `.LNK` and `.OSD` files can be used to import applications.

The menu structure is created in the RES Workspace Manager Console at the **Applications** node. Here you can also make applications available to end users.

There are four ways of creating a menu structure with applications:

- Creating a menu structure by hand and adding applications manually. This can be done by clicking the **New** menu button and selecting **Application** from the drop down menu. The **Edit application** window will open allowing you to enter all application properties manually.
- Adding applications using a Wizard. When clicking the **New** menu button, select **Application (using Wizard)** from the drop down menu to add an application using the Wizard.
- Importing applications with their menu structure to match. With the **Import Wizard** you can import an existing menu and application structure. Of course it is possible to make alterations to the menus to be imported. When importing applications, select **Do not add root folder** to prevent the creation of the folder **Start Menu**. Select **Do not add Programs folder** to prevent the creation of the folder Programs. The folders can be skipped to make the applications fit better in an existing menu.
- A combination of the above.

When you disable an application, you are prompted to provide a message for users who try to start the disabled application. You can also provide such a message on the application's **Notifications** tab (in the application's **Properties** section).

7.3.3 Settings tab

On the global **Settings** tab of **Applications**, you can configure:

- whether managed applications should be fully implemented, partially implemented or disabled.
- additional settings for the behavior of applications and the Start Menu.
- the defaults that should be used for each new application.

RES Workspace Manager managed applications can be implemented fully, partially or not at all. In a new environment, Applications is disabled: **Windows Shell shortcut creation** is set to **Do not create shortcuts**, so that users get the same Start Menu, Desktop and Quick Launch area in their RES Workspace Manager session as they had outside of the RES Workspace Manager session. With this setup, RES Workspace Manager does not manage any of the user's applications. At this point, you can configure applications in the Console, but these are not made available to any users.

When you are ready to start managing users' applications through RES Workspace Manager, you can enable Applications partially or fully:

- To give users RES Workspace Manager-managed applications *in addition to* their existing, non-RES Workspace Manager-managed applications, choose **Windows Shell shortcut creation: Merge with unmanaged shortcuts**.
- To give users *only* RES Workspace Manager-managed applications, choose **Windows Shell shortcut creation: Replace all unmanaged shortcuts**. This eliminates non-RES Workspace Manager managed applications from the RES Workspace Manager session.

 **Note**

If **Windows Shell shortcut creation** (see "**Applications**" on page 87) is set to **Replace all unmanaged shortcuts**, this may lead to unpredictable results for global User Settings that preserve information in `%desktop%`, `%startmenu%` or `%appdata%\Microsoft\Internet Explorer\QuickLaunch`. This does not affect application-level User Settings for those folders.

The following settings determine the behavior of applications and the Start Menu:

Setting	With this setting, RES Workspace Manager will:
Autolaunch new applications on refresh if new application is configured to launch automatically	If access to applications is based on location, and a user starts a Terminal Server session at a certain location, he will have access to the applications that have been configured for that particular location. If the user disconnects from this session and reconnects from a different location, RES Workspace Manager will refresh the Workspace, to update this change. As a result, the user will then have access to the applications that have been configured for the new location. If these applications have been configured for AutoLaunch, selecting this option will automatically launch these applications on a refresh of the Workspace.
Check actively for disabled applications in RES Workspace Manager shell	Check for disabled applications each time the user opens the Start Menu. Disabled applications are marked with a red cross.
Disable Active Setup	ActiveSetup compares registry keys at `HKLM\Software\Microsoft\Active Setup\Installed Components\%APPNAME%` and `HKCU\Software\Microsoft\Active Setup\Installed Components\%APPNAME%`. If the HKCU registry entries don't exist, or the version number of HKCU is less than HKLM, then the specified application is executed by ActiveSetup for the current user. Enabling this option skips the "First Time Shell Init" that occurs, for example, when using mandatory profiles.
Disable autolaunch for managed applications	Select this option to cancel out the autolaunch of any managed application. This overrides the **Autolaunch at session start** option on Application level.
Disable process interception for unmanaged shortcuts	Select this option to disable **Process Interception** (on page 90) globally or for exception tabs. This overrules the application-level setting **If managed shortcut was not used: Intercept new process and apply configuration.**
Do not show offline applications when computer is online	Hides applications if the configured connection state does not match the computer's current connection state. If this option is not selected, users who try to start an "offline" application will be confronted with a message.
Do not show online applications when computer is offline	Hides applications if the configured connection state does not match the computer's connection state. By default, "online" applications are always shown in the user's Start Menu. When a user launches an application, the connection state of the computer is only checked against the required connection state of the application. This allows the user to change the connection state of the computer (by connecting to the corporate network), to gain access to the application without having to refresh the Start Menu. If this option is not selected, users who try to start an "online" application will be confronted with a message.
Do not show Workspace Extensions when VDX / Workspace Extender not detected	Hides applications configured to run as a Workspace Extension on computers on which the Workspace Extender has not been installed.
Refresh start menu if new software is installed	Enabling this option will refresh RES Workspace Manager sessions that use the application shortcut mode **Merge with unmanaged shortcuts** whenever the content of the common Start menu changes due to an (un)install of a software package. As a result, the user's Start menu will reflect this change. After a software package installation has finished, it may take up to 5 seconds before the refresh is performed. This option is not available when **Windows Shell shortcut creation** is set to **Do not create shortcuts** or **Replace all unmanaged shortcuts**.
Remove empty menus	Enabling this option will automatically hide any empty menus from the user's start menu.

Setting	With this setting, RES Workspace Manager will:
When offline, start a specific application () instead of RES Workspace Manager taskbar and **When online, start a specific application () instead of RES Workspace Manager taskbar**	Start a specific application if the connection state of a computer is "Offline", or if it is "Online". These two settings allow you, for example, to configure a laptop to connect to a published RES Workspace Composer when online and to a local RES Workspace Composer when offline. You can specify which application should start: ▪ By clicking the browse button and selecting it or by entering its ID. (You can find this ID on the application's **General** tab). ▪ By specifying an environment variable, in which you have specified the application ID as its value. The application ID or environment variable that you specify will be shown between the brackets. It is possible to configure an application timeout and configure the sessions behavior if the application is terminated before the set timeout, or when the application exceeds the set timeout. By checking **Launch before other actions** the application will be run before other actions are performed, except for RES Automation Manager Tasks and Execute Commands, if these have also been configured to 'run before other actions'.

Note

In a user session, if a user starts an application using **Run as different user**, only the settings that are related to the start of the application (configured on the **Properties > Settings** tab of the application), are applied. These settings are:

- Startup style of application
- Process priority of application
- Disable file system redirector on 64-bit systems

Actions configured for the application (on the **Configuration > Actions** tab of the application) will not be applied.

Process Interception for unmanaged shortcuts

RES Workspace Manager can intercept processes that are started through unmanaged shortcuts, and treat them as if they were a managed application. Process interception for unmanaged shortcuts detects the start of a process, and checks whether a managed application is available to the user that also uses the same process. If such a match is found, all the settings and configurations for the managed application are applied before the process is allowed to continue.

For example, in a session where Microsoft Word is available as a managed application, a user finds and double-clicks an unmanaged shortcut to Microsoft Word. This launches `winword.exe`, which RES Workspace Manager intercepts. RES Workspace Manager first checks that Microsoft Word is allowed to start, based on time restrictions, maximum number of instances, licensing etc. If so, RES Workspace Manager applies the settings and actions configured for Microsoft Word, such as User Settings, Drive and Port Mappings and Environment Variables. As a result, Microsoft Word starts up, and it has all its familiar RES Workspace Manager configurations for the managed application Microsoft Word.

Configuration

On the **Settings** tab at **Composition > Applications**, the option **Disable process interception for unmanaged shortcuts** determines whether RES Workspace Manager will intercept any processes at all. This option can be set for the global Workspace Model and for Workspace exceptions.

To start using process interception, clear the global option **Disable process interception for unmanaged shortcuts**, then configure individual managed applications to intercept their processes if started unmanaged. This is determined by the option **If managed shortcut was not used** (on the application's **Properties > General** tab, under **Automatic shortcuts**):

- **Ignore**: Take no additional action. This is the default setting. The process will start without any configuration by RES Workspace Manager.
- **Intercept new process and apply configuration**: Intercept the process and apply the configuration defined for the managed application.

If a process is intercepted that matches several available managed applications, RES Workspace Manager applies the settings and configurations of the first managed application it finds. This may occur if multiple configurations of the same Managed Application exist.

If a user starts several processes that are intercepted, they are processed one at a time.

A process started from an unmanaged shortcut will continue without any RES Workspace Manager configurations in the following situations:

- if there is no managed application available in the user session for the same process.
- if the managed application is not configured to intercept.
- if process interception for managed shortcuts is disabled.

Process interception for Citrix published applications

To use Process interception for Citrix published applications, set the option **Run RES Workspace Composer** to **Automatic** for servers running XenApp (at **Administration > Agents**). If an unmanaged Citrix published application is started on these servers, it will always be launched by the RES Workspace Composer. If there is a managed application that uses the same process and that is configured with **If managed shortcut was not used: Intercept new process and apply configuration**, it will be intercepted.

To intercept unmanaged Citrix XenDesktop 7 delivered applications, set the registry value `XenDesktop7Intercept`. See the RES Workspace Manager Administration Guide for more information.

Notes

- If the Managed Application Security setting **Only RES Workspace Manager is allowed to launch this application** is selected (on the application's **Authorized Files** tab), users will only be able to start the process using managed shortcuts. This will prevent process interception from taking effect.
- Process interception for unmanaged shortcuts is not supported for virtualized applications such as Citrix XenApp Streaming, Microsoft App-V 4.x and VMware ThinApp.
- When using process interception for unmanaged shortcuts, application environment variables cannot be used in the **Target** field of the unmanaged shortcut to the application.
-

Defaults for new applications

New applications are created with certain default settings, for example for Access Control type, maximum number of instances, etc. You can edit a number of these application defaults to reflect the configuration that is most commonly used in your own RES Workspace Manager environment.

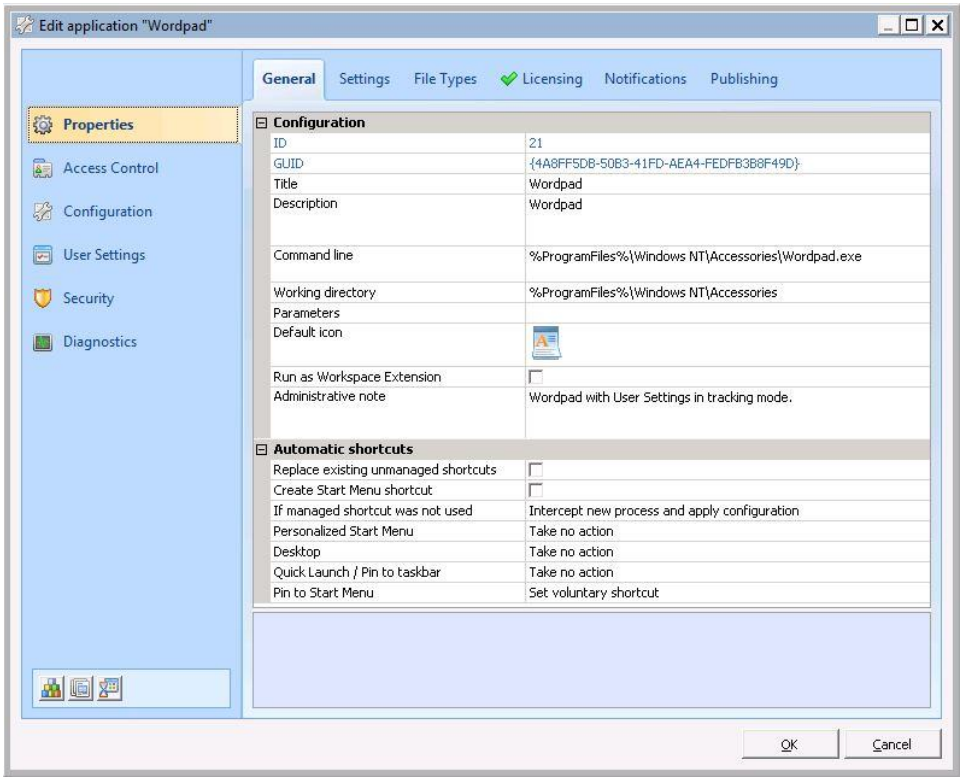
- Click **Set** to configure the defaults for new applications.
- Click **Reset** to revert to the RES Workspace Manager defaults for new applications. Resetting the defaults for new applications does not affect existing applications. It does not affect the other options on the **Properties** tab of the **Managed Applications** node either.

7.3.4 Configuring Applications

Properties

General

When you finish the wizard, the window **Edit Application** will open at the **General** tab of the **Properties** section. Here you can review and edit the settings that have been configured for the application. If you add an application without the wizard, these settings must be configured manually.



The following settings can be configured:

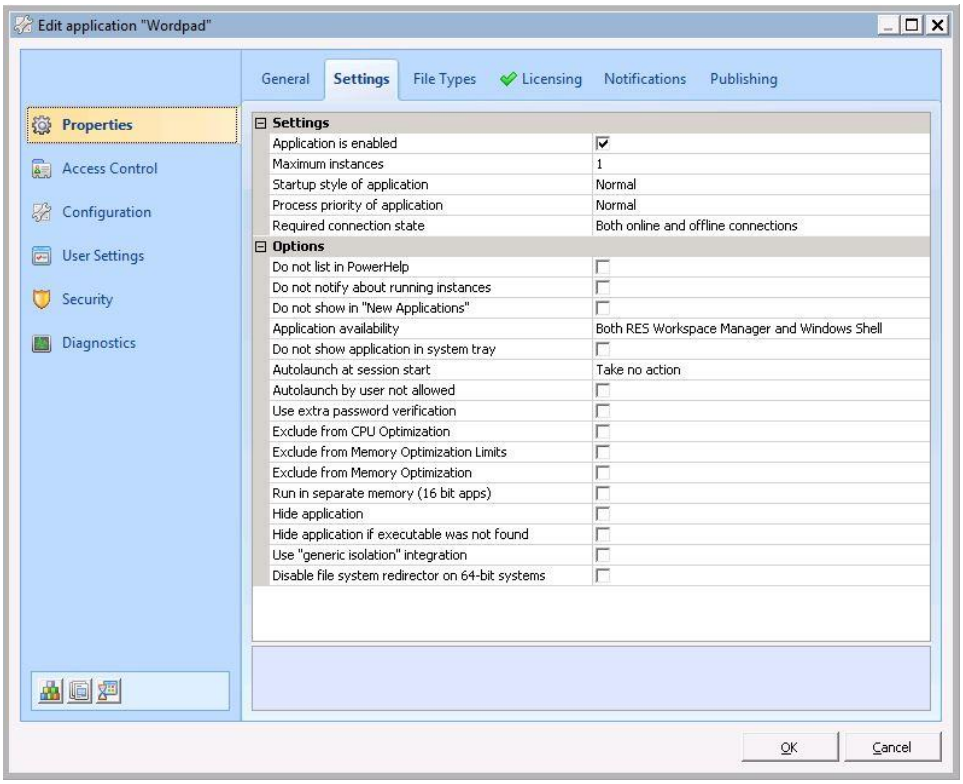
- A clear **Title** and **Description**, and the correct **Command line**.
- If necessary, you can add the **working directory** and **parameters**.
- You can change the application's **icon** if you wish. RES Workspace Manager differentiates between **Default** icons and **Custom** icons. When a default icon is used, RES Workspace Manager will automatically use the high quality icons contained in the application executable (Microsoft Windows Vista and higher only). Applications configured with custom icons will keep their custom ("low quality") icons.
- If the application is installed locally on a workstation and has to be started from a RES Workspace Manager session running on another machine, select the option **Run as Workspace Extension**.
- **Automatic shortcuts** for the application's icons on the Start Menu, Desktop and QuickLaunch bar.
  - Select **Replace existing unmanaged shortcuts** to ensure that the user's Workspace contains only managed shortcuts, no unmanaged shortcuts to the same application. This setting is only applicable if **Windows Shell shortcut creation** is set to **Merge with unmanaged application shortcuts**.

- **Create Start Menu Shortcut** is enabled by default. Disable this option to exclude the application from the user's Start Menu, and to prevent the user from adding such a shortcut using the Workspace Preferences tool.
- To determine the behavior of the application **If managed shortcut was not used** (for example, if an application was started by double-clicking the application .exe), select **Intercept new process and apply configuration** to treat the new process like a managed application applying:
    - User Settings
    - Actions
        - Drive and Port Mappings
        - Drive Substitutes
        - Folder Synchronization
        - User Home Directory
        - User Profile directory
        - Printers
        - User registry / policy
        - Execute Command Automation Tasks
        - Environment Variables
    - E-mail Settings
    - Data Sources
    - Application Notification (only for enabled Applications)

The default setting at **If managed shortcut was not used** is **Ignore**. An ignored process will remain unmanaged.

Settings

When you have set up the basic configuration of an application you can use the **Settings** tab to configure some additional options.



- The option **Application is enabled** is selected by default. Clear the option to disable an application.
- To preserve system capacity, you can set a maximum on the number of application **instances** allowed. If you set **Maximum instances** to one, the user will be able to start only one instance of the application. If **Maximum instances** is set to more than one and the user tries to start the same application for the second time, he will be offered a choice to switch to the running instance of the application or to start a new instance. If this setting is left at zero (the default setting), there is no cap on the number of instances of an application. A value ranging from 0-30 can be specified as maximum # of instances.
- You can set the startup style of the application as **Maximized** (which is the default), **Normal**, or **Minimized**.
- With the option **Process priority of application**, you can choose the process priority of the application. Assigning a high priority to an application means the application will be allowed to use a large amount of processor capacity, possibly resulting in system hiccups or even system freezes. A low priority means less chance of system freezes, but may make the application slow.
- With the option **Required connection state**, you can define the connection state(s) that the application requires in order to function. If this connection state is not detected, the application cannot be started, and a message will be displayed. This is useful, for example, for applications on laptops, or in a dial-up situation.
- Several options can be set at the **Options** section. For an explanation of these specific settings, see the RES Workspace Manager Help (available from the Console by pressing F1).

File Types

You can manage Windows file type associations with the RES Workspace Manager File Type technology.

If an application is associated with a file extension, a green check mark will appear next to the File Types caption.

Whenever a Managed Application is created, an exclamation mark is visible on the **File Types** tab caption, notifying you that no File Types have been configured for this application yet. After closing the application this exclamation mark will disappear, indifferent of whether File Types have been configured.

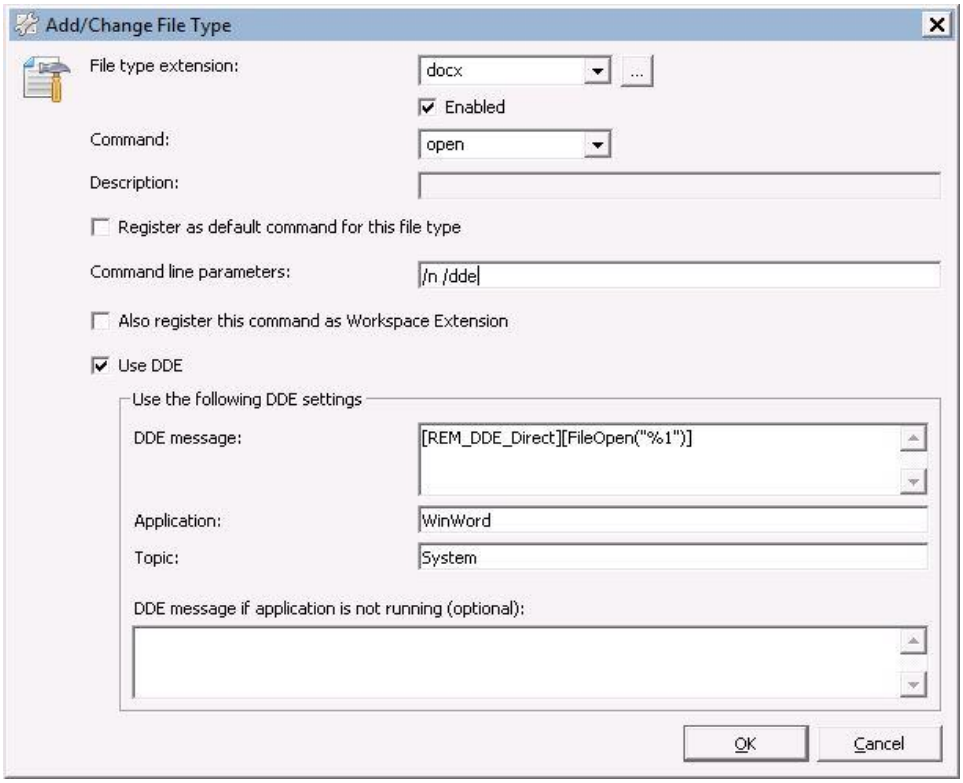
At the File Types tab the following options are available:

- **Add**: adds a file association to the application
- **Edit**: edits the file association
- **Delete**: deletes the file association

The same file type and command may be entered for more than one application. For example, WordPad can open simple `.doc` files, but Microsoft Word also supports this file type. To determine what should happen if a user has access to both applications, assign an application priority to the file type/command. You can do this in the **Properties > File Types** window when editing the application, or on the **File Types** node of **Composition > Applications**.

The application at the top of the priority list for a certain file type or command will handle the file type association. If this application is not accessible to the user, the second application on the list will be used, and so on. If the initial application that handles a certain file type and command is temporarily not available (that is, disabled or limited by Time Restrictions), RES Workspace Manager will look for an alternative application. This alternative must be configured for the same file type/command and must also be available in the user's menu.

When you add or edit an association, you can configure the following options:



- **File type extension**: the extension to be associated with an application. Select a known association with the browse button or enter a new extension manually.
- **Enabled**: whether the association is to be enabled.
- **Command**: the command associated with the file type (for example "edit", "open", or "print"). Usually executed by Windows when a user double-clicks a file from the Explorer or when a file is launched from another application. The command (or its description) will show in the context menu when right-clicking a file in the Explorer. Select a known command with the browse button or enter a new command manually.
- **Description**: a short description of the command that will be shown in the context menu when right-clicking a file in the Explorer.
- **Register as default command for this extension**: the default command is the command that will be executed by Windows when a user double-clicks a file.
- **Command line parameters**: the command line parameters that should be used for the application when the user selects the command. For example, use "/p %1" when configuring the "print" command for WordPad, so that WordPad will print the selected file.
- **Also register this command as Workspace Extension**: enables support for File Types for the RES Workspace Extender / RES Subscriber.
- **Use DDE**: When you create or import a new application in RES Workspace Manager, RES Workspace Manager automatically selects the option **Use DDE** for the application's File Types that require DDE. The relevant DDE settings are also filled automatically. The list of File Types on an application's **File Types** tab includes a column that shows which file associations use DDE. To disable the use of DDE for a particular file type, open it from the list and clear the option **Use DDE**.

  DDE is not automatically used for existing applications in RES Workspace Manager. To start using DDE for an existing application, re-import the application's file types. Open the application, go to **Properties > File Types** and click **Import**. This replaces any existing file types with the machine default file types, and all relevant File Types will be configured to use DDE with the relevant DDE settings. If necessary, you could also manually enable DDE and configure the relevant settings, but re-importing the File Types is normally faster and safer.

Notes

- You may use special file types. These file types (mailto, http, ftp, nntp, and news) are not actual file types, but determine what should happen when a user clicks a mail link in Internet Explorer, or when a user clicks an Internet URL in an e-mail message. By configuring these file types for an application, you have total control over which applications are started for these actions.
- RES Workspace Manager does not store its DDE info in the user's registry like Microsoft Windows does.

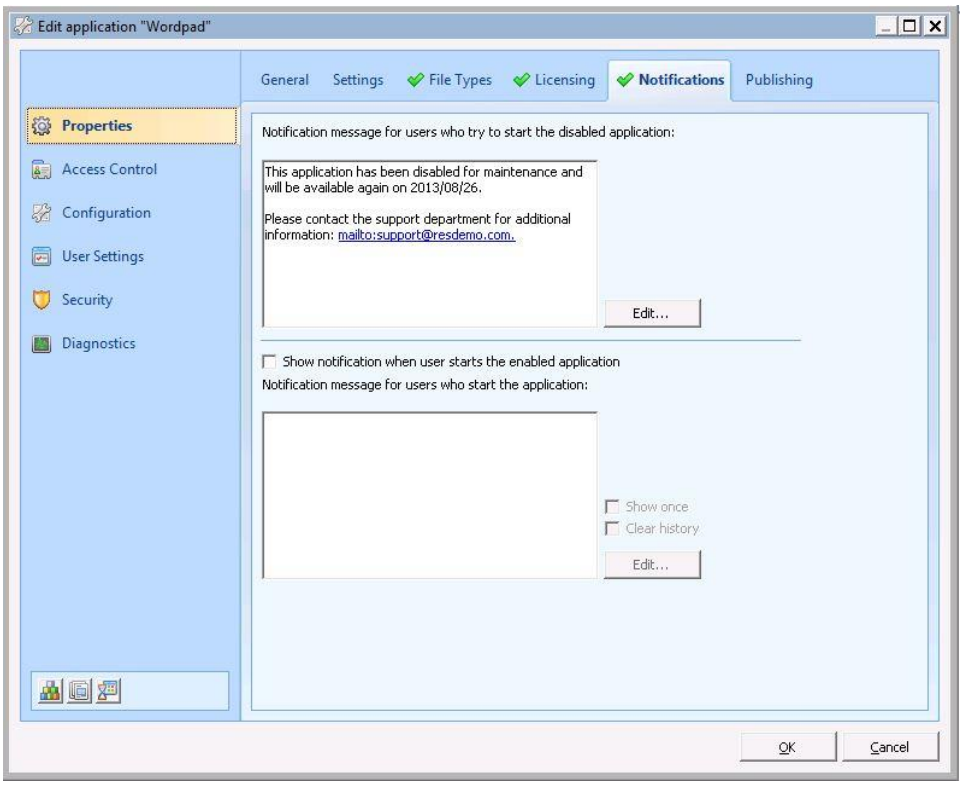
If you have configured a File Type for an application, you can use **PF_IFA** in the application's **command line parameters** to indicate where the filename should be inserted.

For example, if you have configured the command line for Microsoft PowerPoint as "`/splash`" to suppress PowerPoint's splash screen, double-clicking a `.ppt` file will result in an attempt to launch PowerPoint with the command line "`/splash h:\somefile.ppt`". This will not work, because PowerPoint requires the filename to be the first parameter. Instead, specify "`$PF_IFA$ /splash`" as the application's command line. When the application is launched through a File Type Association, the filename will no longer be appended to the application's command line, but instead will be inserted in the position indicated with `$PF_IFA$`. When the application is launched directly from the menu, the `$PF_IFA$` text will be removed.

It is also possible to use **$PF_IFA_REPLACE$** in the application's command line parameters to indicate that the command line should not be used at all when the application is launched through a File Type, but that only the filename should be passed to the application through the File Type.

Notifications

At the **Notifications section** you can set up a message for users when they start the application: one for if it is **enabled** (which you can also set to be displayed only once), and one for if it is **disabled**.



- For enabled applications, you could use this message to provide useful information about a newly available application.
- For disabled applications, the message could explain why the application has been disabled, and for how long.

Notes

- The notification messages support `.rtf` format and can contain hyperlinks (e.g. `mailto:`, `http://`, `file://`).
- The size of the **Edit notification** window determines the size of the notification window as it will be displayed to the user.

Licensing

Use the **Licensing** tab to configure application license metering. By managing the application license usage of Managed Applications, you can enforce license compliance to e.g. Microsoft licensing models.

It fully depends on the type of software license whether or not preventing access is enough for license management. The method of preventing access must comply with the type of software license. Here is an overview of the license types that RES Workspace Manager can enforce. This enforcement is done on top off the access management of the application (i.e. a user may be granted access based on a distribution group, but the license enforcement may prevent the application from being used).

Concurrent user licensing

This type of licensing is uncommon for Microsoft applications. RES Workspace Manager keeps track of the number of unique users that simultaneously use the same application. If the threshold is reached then no additional users can launch the application. The maximum number of concurrent users as well as the users that used the application can be tracked for later reporting.

Named user licensing

This type of licensing is uncommon for Microsoft applications. RES Workspace Manager keeps track of the number of unique users that used the same application. If a new unique user tries to launch the application while the threshold is reached then the application will not be accessible. A list of unique users is maintained (including the denied users). Also the users that used the application can be tracked for later reporting.

Seat licensing

This type of licensing is very common for Microsoft applications. RES Workspace Manager keeps track of the number of unique computers that run the same application. There is an exception: if the application is run on a remote desktop, then the client computer accessing the remote desktop is being tracked instead. If the threshold of maximum allowed seats is reached then no additional new (client) computers can launch the application. A list of unique seats is maintained (based on domain and computer names) including the denied seats. Also the users and computers that used the application can be tracked for later reporting.

How to configure application licensing

1. Open the application and click **Properties > Licensing**.
2. Select the application license type in the **License type** field and configure the selected application license type:
   - **Company wide license**: unlimited access for all users.
     1. Enter the license cost in the **License cost** field.
     2. Enter the number of licenses in the **# of licenses** field. This will automatically calculate the total cost of licenses in the **Total cost** field.
     3. In the **Max. # of users** field, enter the maximum number of users that can be granted access to the application. This field is only available if access to the application is managed by application managers. See Configuring access to an application based on identity.

- **Server license**: access is based on server licenses. If all server licenses are in use, access will be denied to additional users and a message will be shown instead.
  1. Enter the license cost in the **License cost** field.
  2. Enter the number of licenses in the **# of licenses** field. This will automatically calculate the total cost of licenses in the **Total cost** field.
  3. In the **Max. # of users** field, enter the maximum number of users that can be granted access to the application. This field is only available if access to the application is managed by application managers. See Configuring access to an application based on identity.
- **Per seat license**: access is based on seat licenses. By linking licenses to client names instead of users, RES Workspace Manager can enforce seat licenses for desktops and laptops, but also for Thin Clients. At **#of licenses**, click  to set seat licenses per Zone.
  1. In the field **If database connection not available**, specify the license metering behavior if there is no connection to the Datastore and the actual number of licenses or seats cannot be determined.
     - **Always grant access** (default): access to the application will always be granted and the claimed license will be cached to be processed later. You can change the default setting for new applications in the node **Composition > Applications** at the **> Properties** tab.
     - **Do not grant access**: to force compliance with the configured licensing options, access to the application will be denied if a Datastore connection is not available.
  2. Enter the license cost in the **License cost** field.
  3. Enter the number of licenses in the **# of licenses** field. This will automatically populate the **Total cost** field with the total cost of licenses.
     - Click  to configure the number of seat licenses per Zone. This will open the **Seat licenses per Zone** window.
  4. In the **Max. # of users** field, enter the maximum number of users that can be granted access to the application. This field is only available if access to the application is managed by application managers. See Configuring access to an application based on identity.
  5. Click **Seats** to view the number of seats currently in use and the users that have claimed them. This button is only available if the application uses seat licenses.
- **Per named user license**: access is based on specified users. If all licenses are in use, access will be denied to additional users and a message will be shown instead. If access is managed by an application manager, this message will be shown to him.
  1. Enter the license cost in the **License cost** field.
  2. Enter the number of licenses in the **# of licenses** field. This will automatically populate the **Total cost** field with the total cost of licenses.
  3. In the **Max. # of users** field, enter the maximum number of users that can be granted access to the application. This field is only available if access to the application is managed by application managers. See Configuring access to an application based on identity.
  4. Click **Named users** to view which users have access to the application. You can configure access to the application on the **Access Control** tab. If you have delegated access to the application to an Application Manager, the **Information about users and applications** window will open, which shows information about the application and the users with access to it.

- **Per concurrent user license**: access is based on concurrent users. If you use this license type, you cannot configure the **Maximum instances** of the application on the **Settings** tab. Concurrent user licenses are supported for desktops and server-based computing environments. If all licenses are in use, access will be denied to additional users. Instead, a message will be shown, together with a list of current users. This avoids the purchase of needless user licenses, because it allows users to arrange access to the application among themselves. RES Workspace Manager will automatically retry to claim a concurrent license after 30 seconds. Users can use the **Retry** button to speed up this process.

  1. In the field **If database connection not available**, specify the license metering behavior if there is no connection to the Datastore and the actual number of licenses or seats cannot be checked.
     - **Always grant access** (default): access to the application will always be granted and the claimed license will be cached to be processed later. You can change the default setting for new applications at **Composition > Applications > Managed Applications > Properties**.
     - **Do not grant access**: to force compliance with the configured licensing options, access to the application will be denied if a Datastore connection is not available.
  2. In the field **Idle timeout in minutes**, specify how long the application can remain inactive before it is forcibly closed by RES Workspace Manager. Because an inactive application unnecessarily holds a lock on a concurrent user license, selecting this option is useful if the number of available licenses is limited. If an application is forcibly closed, this will be logged in the Event Log of the user.
  3. By default, only the application's main process is closed when the timeout expires. To also forcibly close child processes of the application when the idle timeout expires, select **Force close of child processes**.
  4. Enter the license cost in the **License cost** field.
  5. Enter the number of licenses in the **# of licenses** field. This will automatically calculate the total cost of licenses in the **Total cost** field.
  6. In the **Max. # of users** field, enter the maximum number of users that can be granted access to the application. This field is only available if access to the application is managed by application managers. See Configuring access to an application based on identity.
  7. Click **Concurrent usage** to view which users are currently using the application.

Note

If you select **Per seat license** or **Per concurrent license**, the setting **Only RES Workspace Manager is allowed to launch this application** on the **Security** tab will be selected automatically, to ensure that the user can only start the application via his Start Menu or desktop. This allows RES Workspace Manager to check how many application licenses are in use.

Tip

If the application uses licenses per concurrent user, click **Concurrent usage** on the application's **Licensing** tab to see which users are currently using the application.

Access Control

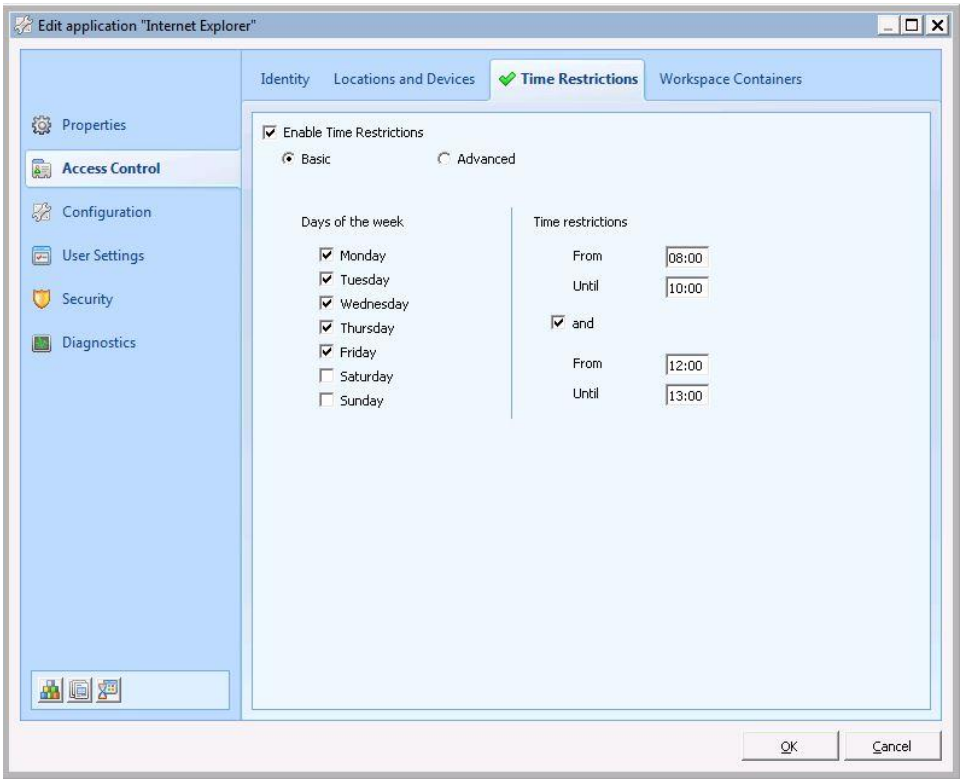
Besides on **Identity**, **Locations and Devices** and **Workspace Containers**, access on applications can also be set on **Time**.

The **Time Restrictions** option enables you to limit application access based on time. This can be very useful when access to an application needs to be restricted. For example, the availability of a database based on the Service level Agreement. Time Restrictions are based on the local time of the user's session.

You can set up time restrictions on the **Time Restrictions** tab of the application's **Access Control** section.

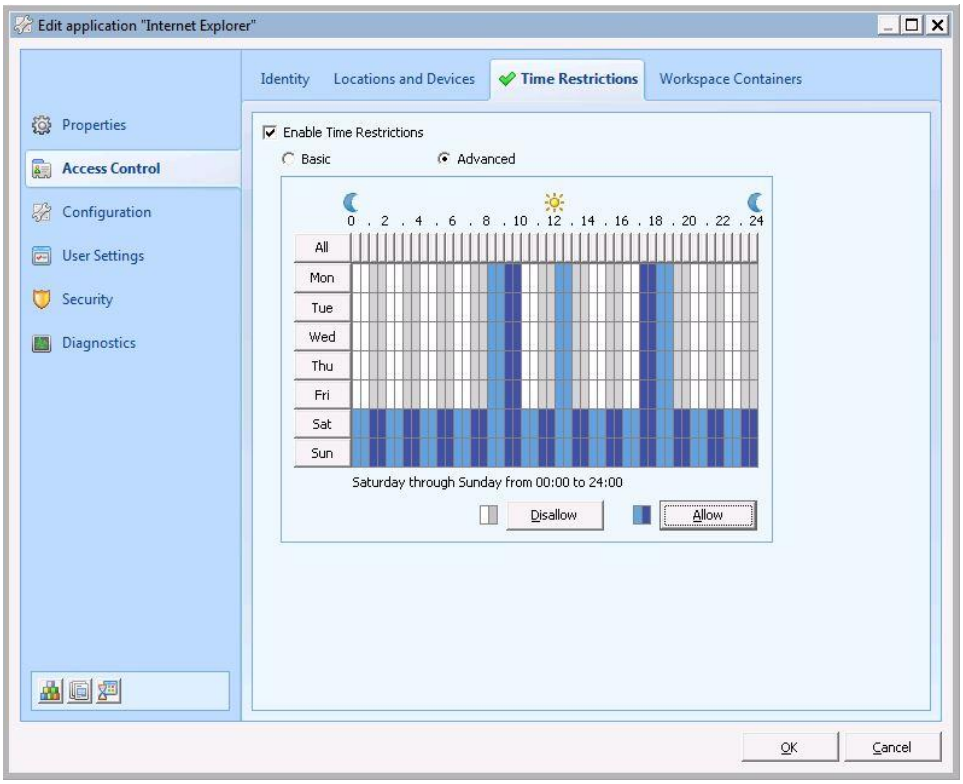
Time restrictions can be set in **Basic** and **Advanced** mode.

In **Basic** mode, you can set the days on which the application may be used, and you can define a maximum of two time spans. When a user tries to start an application outside the allowed hours, it will not run; a message will be displayed instead.



If a user is running an application for which the time of availability has come to an end, a warning message is displayed with a countdown. At the end of the countdown, the application is terminated.

In the **Advanced** mode, a wider variety of possibilities is available for enabling or disabling access to an application.



Select the appropriate time spans per day, and Allow or Disallow access to the application by clicking the appropriate button.

If **Time Restrictions** are enabled, a green check mark will appear in the tab.

Configuration

Actions

On the **Actions** tab you can add specific actions for the application you are editing. These actions will be invoked when the user launches the application. The available actions are virtually identical to these settings that are available in the **Composition > Actions By Type** node of the Console.

- It is possible to **Move** and **Duplicate** settings related to Actions. This makes it possible to:
  - duplicate application settings and move them from one application to another
  - duplicate application settings and move them to a global level
  - duplicate global settings and move them to an application
- It is also possible to implement the Actions configured for another application by adding **Linked Actions**. When adding a linked action, you only need to select the source application that contains the actions to be used. This makes it possible, for example, to create an application with a default set of Actions and to link various other applications to that source application, thereby making it unnecessary to create multiple applications and the same set of Actions for each application.
  - The execution of "Linked Actions" is restricted based on:
    - The Access Control set on the Actions configured for the source Managed Application.
    - The Workspace Control set on the Actions configured for the source Managed Application.
    - Access Control configured for the source Managed Application is ignored.
    - Workspace Control configured for the source Managed Application is ignored.
    - Actions that use the setting **Run Once** are only run once for each user, even if several applications reference the same Action.
- Managed applications can be linked to multiple managed source applications.
- Multiple managed applications (targets) can be linked to a single managed source application.
- Linked Actions cannot be linked to any managed application that already has "Linked Actions" to another managed application.
- Managed Applications cannot be linked to the same managed source application more than once.

Please refer to the section **Actions** for more information about the different Actions avaialble in RES Workspace Manager:

- **Environment Variables**
- **Drive and Port Mappings**
- **Drive Substitutes**
- **Printers**
- **User Registry Setting**
- **User Registry Policy**
- **User Home Directory** (See **Directory Maintenance**)
- **User Profile Directory** (See **Directory Maintenance**)
- **Folder Synchronization**
- **Execute Command**
- **Automation Tasks**
- **Microsoft ConfigMgr**
- **LANDesk**
- **Linked Actions** - It is possible to implement the Actions configured for another application. When adding a linked action the only configuration to be made is selecting the source application, containing the actions to be used.

Notes

- If a user starts the application using his Start Menu (you can enforce this on the Security section when editing an application), the Actions of the application will be invoked and the user's Event Log will be appended with the results of the applied settings. You can view the contents of this Event Log in the Workspace Analysis (see **Workspace Analysis** (on page 241)) window of this user.
- The behavior of Actions for Applications is identical to the before mentioned options. However, the **Fast Connect** option is not available for Network Printers on application level.

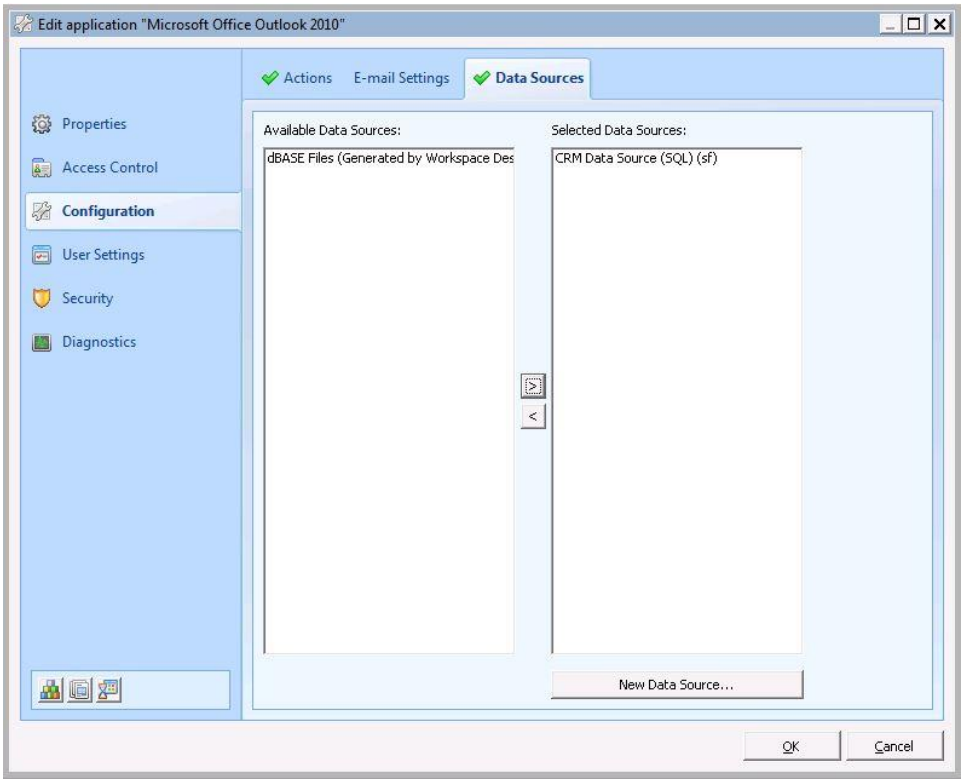
E-mail Settings

To associate the E-mail Settings with one or more mail applications, select a Setting from the list of Available E-mail Settings and then click the > button to move it to the list of Selected E-mail Settings. See **E-mail Settings** (on page 108).

If a Setting is associated with the application, a check mark will be shown on the **Mail** tab.

Data Sources

If you want to link an application to one or more Data Sources, select the applicable Data Sources from the list of Available Data Sources and click > to add it to the list of Selected Data Sources. See **Data Sources** (on page 109).



If an application has been configured to use a Data Source, a green check mark will appear next to the **Data Sources** caption on the tab.

User Settings

Usually, users can change certain settings in a session, such as their default printer, their mouse orientation, and the view in which an application should open.

Applications and processes store such user settings in keys and values in the user-specific part of the registry (`HKEY_CURRENT_USER`), and in configuration files in the user's profile directory. In many environments, however, user profile directories and `HKEY_CURRENT_USER` are not preserved when the user logs off. This is particularly the case if you use mandatory profiles, or if you use roaming profiles in combination with passthrough applications in a Citrix XenApp environment. As a result, users get the default settings again when they log on, instead of the settings they had previously customized.

With RES Workspace Manager User Settings, you can preserve changes that users make to certain settings, files and folders during a session. These User Settings are preserved in the user's home folder, and are restored automatically when the user logs on again.

Configuration

- User Settings can be configured both on the global level (**Composition > User Settings**) and for a specific application (open the application, go to **User Settings > Properties**).
- The User Settings feature must be enabled (at **Composition > User Settings**) for User Settings to work at any level.
- You can select **Use the User Settings from the following application** to link an application to the User Settings of another application, rather than giving the application its own User Settings. Please note that linked User Settings are not supported for Citrix Streamed Applications/Microsoft App-V 4.x applications.
- For more information, please refer to User Settings (global).

Note

With User Settings tracking for applications, in a mixed environment of RES Workspace Manager Console 2012 SR2 or higher and RES Workspace Composer 2012 SR1 or earlier, subfolders of %LOCALAPPADATA%, e.g. %LOCALAPPDATA%\Microsoft, will not be tracked.

7.3.5 File Types

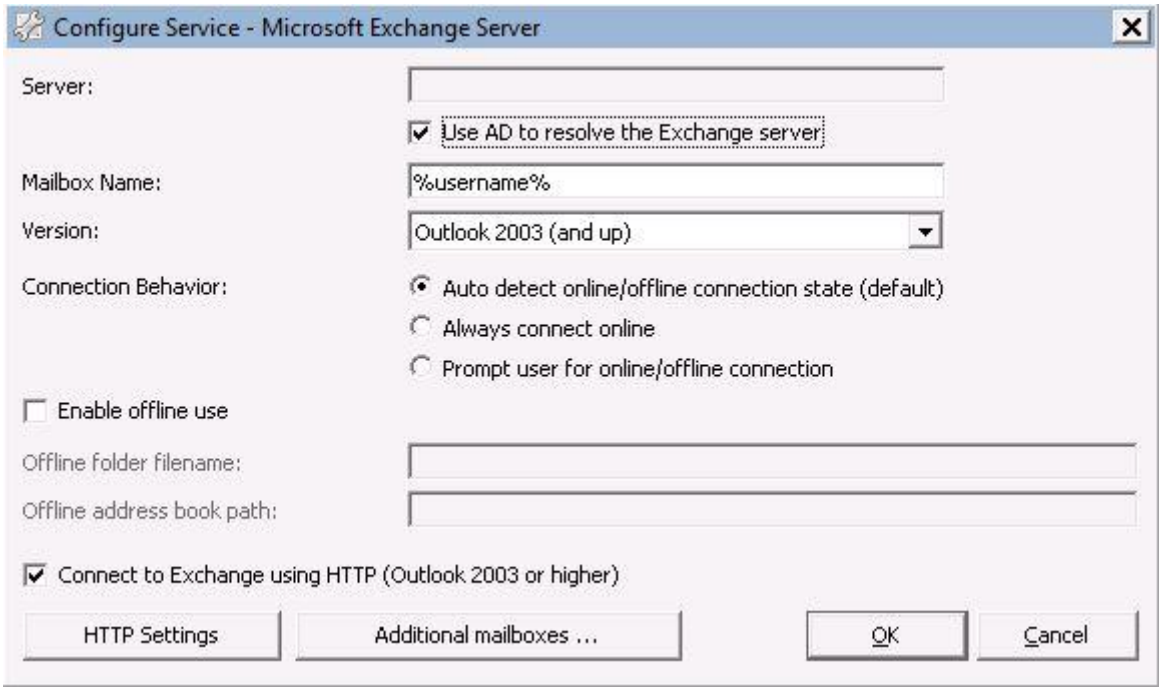
On the **File Types** section you can view all file extensions and their associated programs. By clicking the **Edit** button, the priority of the associated programs can also be modified here, in the same way as on the **File Types** tab of the **Configuration** section of an application.

7.3.6 E-mail Settings

An **e-mail profile** stores various types of information. This can include information that users need to access mail servers, provider(s), personal address book storage, or a personal information storage. With **E-mail Settings** you can configure mail profiles in an easy and flexible way.

Each user who needs to use a MAPI-compliant e-mail client (for example Microsoft Outlook) needs a **mail profile**. Normally, this would require manual configuration or advanced scripting techniques. With E-mail Settings you can preconfigure and manage various mail profiles for all users from a single point of administration, without any programming or scripting.

To create an E-mail Setting, go to **Composition > Applications > E-mail Settings** and click the **New** button. Simply enable and configure the services you would like to include in the E-mail Settings by clicking **Configure**.



Moreover, a **Create once** option is available. This option will create a mail profile:

- when a user starts the mail application for the first time;
- if a mail profile does not exist; or
- if **Clear history** has been used.

By combining **Create once** and **Clear history**, migrations to new mail servers and/or clients are easily orchestrated from one console.

Note

Refer to the manufacturer for information on the configuration of a service. Contact RES Software at support@ressoftware.com for additional services.

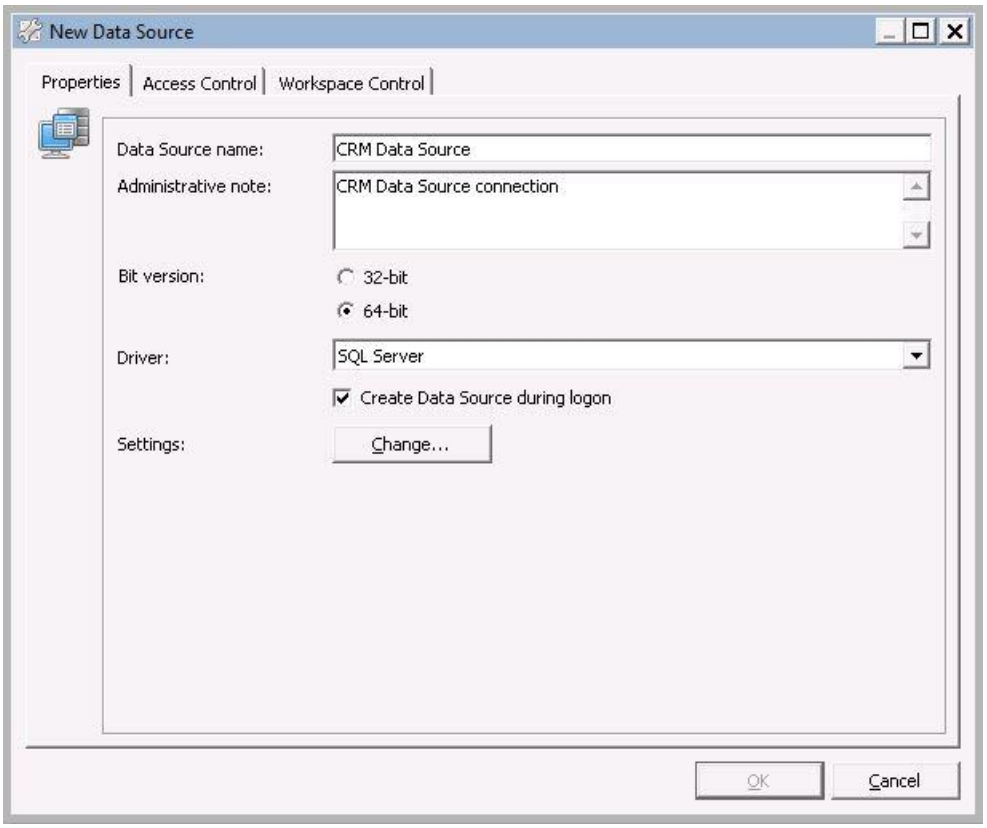
7.3.7 Data Sources

Open Database Connectivity (**ODBC**) provides a common layer between Windows applications and their databases.

After installation of the ODBC drivers on the relevant technology stack, the applications will need to connect to their databases. This connection is usually established by creating a link on the desktops, laptops and Terminal Servers to the database servers and the necessary databases (**DSN** or Data Source Name). For example, on each workstation, laptop, and Terminal Server running the CRM application, you would have to create a link to the CRM database on an SQL database server (the DSN).

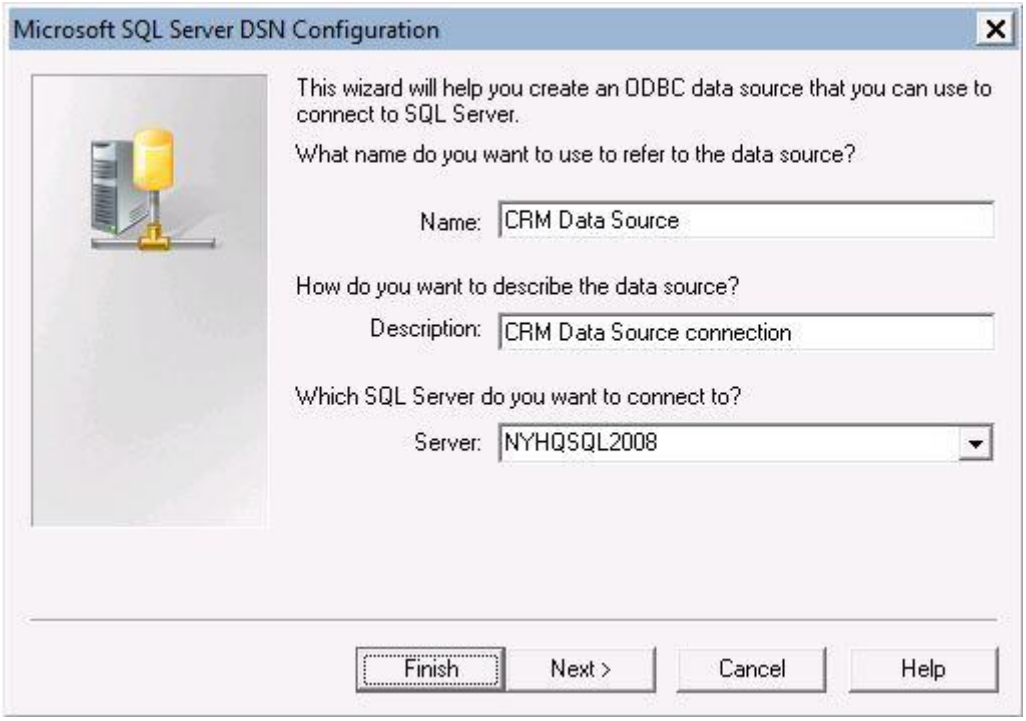
With RES Workspace Manager, you can use the **Data Sources** technology to define the DSN **once**, using a simple Wizard in the RES Workspace Manager Console, and then link the applications that need to connect to it. When the user starts the application, the database connections will automatically be set up and made available for the application. This makes it easy, fast, and reliable to create data sources.

To create a Data Source with the Wizard, go to **Composition > Applications > Data Sources** and click the **New** button in the command bar.



Normally, a Data Source is created in a user session when the application to which it is linked is started. This may cause a delay when starting the application. It can therefore be useful to select **Create Data Source during logon**.

When you have added the Data Source, click **Change** and complete the Configuration wizard.



Tip

By clicking **Workspace Designer** it is possible to use the Workspace Designer to create Data Sources based on your current environment. This enables you to easily transfer from a non-managed environment to a RES Workspace Manager managed Workspace. For more information, see Desktop Transformation.

7.3.8 Workspace Extensions

RES VDX enables the integration of locally installed applications into Centralized (Server Based) Computing RES Workspace Manager environments. This makes it possible to manage and control the access to local applications as well as Terminal Server applications from one central point: the RES Workspace Manager Console.

Configuring Workspace Extensions

Workspace Extensions are applications that are managed centrally with the RES Workspace Manager Console. If you configure an application to run as a Workspace Extension, it will be displayed in the RES Workspace Manager menu like any other application. The only difference is that you need to specify the local path on the client for the application.

To run an executable on a local workstation as a Workspace Extension in a Centralized Computing session (for example a CAD program), complete the following steps:

- Install the RES VDX Client plugin on the client.
- Create an application with the RES Workspace Manager Console. Select the option **Run as Workspace Extension**.
- Test the configuration by starting the Application.
- Check Usage Tracking to see whether the application usage is logged.

You may also associate the application with a **Zone**:

- Open the Application's properties in the RES Workspace Manager Console.
- Add a Zone at the **Access Control** > **Locations and Devices** tab.
- Select a previously created Zone or create one.

This restricts the Workspace Extension to a specific Zone. This can be useful, for example, if the application is not locally installed on all workstations. As an alternative, assign the application to a specific **Workspace Container**.

Integrating File Types with Workspace Extensions

File Types seamlessly integrate with Workspace Extensions.

If you configure a File Type and select **Also register this command as Workspace Extension**, the File Type will also be registered on the client using the Workspace Extender (provided that your environment uses the Workspace Extender).

- If the user runs an application configured to run as Workspace Extension and accesses a file that is associated with an application that is located on a Terminal Server, RES Workspace Manager will automatically open this application. For example, if you have configured Microsoft Outlook to run on a Terminal Server and associate it with the "mailto" special file type, RES Workspace Manager will automatically open Microsoft Outlook in the Terminal Server session if the user opens a mail link in Internet Explorer that runs locally.
- If you have configured a File Type for a Workspace Extension and the user double-clicks this file type in the Terminal Server session, RES Workspace Manager will automatically start the associated Workspace Extension and open the selected file (or resource). For example, if you have associated the file type "http" with the Workspace Extension Internet Explorer and the user double-clicks an Internet URL from any application in the Terminal Server session, RES Workspace Manager will start the Internet Explorer which was configured to run as Workspace Extension.

In both cases, the files (or resources) must be available on the Terminal Server AND the local client. For example, if the user double-clicks a PDF file on a network share that has been mapped with drive letter "T:" and you have associated this file type with an application configured to run as Workspace Extension on the client, the same drive letter "T:" must be accessible on the client.

You can view the location of both file and application in the **File Types** node of the **Workspace Analysis** window of a specific user, which can be accessed through the node **Diagnostics** > **Workspace Analysis**. In this way, it is always clear how the redirection of File Types takes place between RES VDX and RES Workspace Manager.

7.4 Actions

Use Actions to configure global actions, or specific actions for an application. Global actions are executed at the start of the user session, application actions when a user launches an application. Application actions will be invoked whenever a started application is managed by RES Workspace Manager. This is the case if the application is started from the Start Menu or when the application is started by a configured File Type. Applications are not managed by RES Workspace Manager if they are started from a command prompt, directly started from the Windows Explorer or from the run command. This can be prevented by selecting **Only RES Workspace Manager is allowed to launch this application** at the **Security > Authorized Files** tab of the application.

The user's Event Log will be appended with the results of the applied settings. You can view the contents of this Event Log in the Workspace Analysis window of this user.

Actions can also be configured on a global level.

- The behavior of Actions for Applications is identical to the before mentioned options, except:
- **Hide Drive** behavior is not available in Drive Mappings.
- The option **Set as default printer** for Network Printers is mandatory, but this will not reset the user's preference. The next time the user logs on, the preferred default printer will be restored. The user will also be notified of this event by his Printing Preferences tool.
- The **Fast Connect** option is not available for Network Printers.

It is possible to **Move** and **Duplicate** settings related to Actions. This makes it possible to:

- duplicate application settings and move them from one application to another
- duplicate application settings and move them to a global level
- duplicate global settings and move them to an application

Please note that executing an action on session reconnect requires an RES Workspace Manager refresh. Therefore, when configuring actions to be executed at session reconnect, make sure the option **Do not refresh Workspace when reconnecting to a session** is *not* enabled (at **Composition > Lockdown and Behavior**, in the **Workspace Composer** section).

7.4.1 Drive and Port Mappings

It is possible to create **drive and port mappings** based on all previously mentioned types of access control.

There may be hundreds of network locations and ports (lpt/com) available: rather than browse a list every time you need a specific one, you can "map" it. This sets your machine to connect to it when you log in and treat it like one of its own disk drives or ports.

Configuring Drive and Port Mappings

Global settings

- **Disconnect all network drives before logging on/off** cleans the user's profile from user-connected and disabled drives.
- **Skip unmanaged drives** can only be selected when the option **Disconnect all network drives before logging on/off** is enabled. Only network drives that are managed by RES Workspace Manager will be disconnected, all other drives will not be touched. With an unmanaged drive, a drive is meant that has no managed equivalent in RES Workspace Manager. If both a managed and an unmanaged version of a drive exist, the unmanaged version will be replaced by a managed version after logging off/on.
- **Refresh Drive and Port Mappings when network connectivity changes** allows you to refresh Drive Mappings automatically when the network connectivity of a session changes. This ensures that connection state-dependent Drive Mappings become available or disappear correctly.

  Drive and port mappings will *not* be refreshed if the Lockdown and Behavior option **Do not refresh Workspace when network connectivity changes** is selected (at **Composition > Desktop > Lockdown and Behavior**).

- **Also connect all network drives using VDX plugin**. Drive mappings that are configured for the remote desktop can be set as local drive mappings too. This setting enables the user to access the same drives from local desktop and from virtual desktop using the VDX plugin.
- You can override the global settings of this feature for specific Workspace Containers.

Mapping settings

- Optionally enter a note in the **Administrative note** field. This is useful to differentiate the mappings that you configured.
- **Action**:
- **Map drive**: Default; perform drive mapping
- **Disconnect drive mapping**: Disconnect an existing (non-RES Workspace Manager) mapping.
- **Do not perform mapping operation**: Do not perform the actual mapping, but do set other options, such as setting a friendly name. This setting is also useful when configuring hide drive behavior for existing local drives.
- **Set RES HyperDrive**: perform drive mapping to an existing RES HyperDrive as specified in **RES HyperDrive Fileserver name**. This setting is only available if **RES HyperDrive integration** is enabled (at **Setup > Integration > RES Software > RES HyperDrive**). When selecting this setting, unavailable settings for this mapping are greyed out.
- The **Device** field specifies which drive letter should be used for the mapping.
- If you select **Do not use a drive letter**, RES Workspace Manager will not expose the drive letter when a mapped network resource should be available for the user.
- If you select **Find first free drive letter**, RES Workspace Manager will find the first available drive letter when mapping a network drive, starting down from "Z:".
- The **Hide drive** field specifies the hide drives behavior of the mapping. Hidden drives are not available to end users and are also blocked in Windows Explorer-type dialogs.
- If you select **Default**, the default hide drives behavior for Drive and Port Mappings will be applied.

- If you select **Always hide, but allow access**, the drive will be hidden without blocking it. This can be useful for removable media that cause a delay in application startup or File Open/Save dialogs.
- **Fast connect** allows users to start their sessions faster. Do not select this option if the drive contains applications: until the user accesses the drive, the drive will not be available, which means that any applications on the drive will not be available either.
- When selecting the option **Fast connect**, the option **Wait for task to finish before continuing** becomes unavailable, because the actual mapping will first be performed when the user connects to the drive.
- When clearing the option **Wait for task to finish before continuing** the option **Fast connect** becomes unavailable, because the task will be performed asynchronously.
- The **Required connection state** field specifies the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an online connection state.
- Click the **Access Control** tab to configure the Access Control criteria of the mapping.
- Click the **Workspace Control** tab to configure to which Workspace Container(s) the mapping applies.

Notes

- You can use environment variables (for example, %username%).
- For additional security, Drive and Port mappings can also direct the drive mapping to a resource, without the user knowing the username or password.
- On Microsoft Windows Vista or later, Drive and Port Mappings also allow mappings to WebDAV web folders, which start with "http://" or "https://" instead of "\\server\share".
- WebDAV mappings to RES HyperDrives connect to the Fileserver without the use of the RES HyperDrive Client. As a result, files and folders are not cached locally.
- Use the **Workspace Analysis** window to display an overview of all mappings and their hide drive settings for a specific user.

Default Hide drives behavior

Hidden drives are also blocked in Windows Explorer-type dialogs.

- **Disabled**: No default hide drives behavior is configured.
- **Never hide any drives**: Overrides any hide drive settings in **Drive and Port Mappings**.
- **Do not hide any drives (unless otherwise specified)**: Default behavior is to show all drives. This setting is overruled by any hidden drives configured with **Drive and Port Mappings**.
- **Hide all drives (unless otherwise specified)**: Default behavior is to hide all drives. This setting is overruled by any drives configured to be shown with **Drive and Port Mappings**.
- **Never Hide Home Drive** is selected by default. If selected, the user's home folder will never be hidden, regardless of the Hide Drives setting of individual mappings.

Create a drive mapping using information from Active Directory

Active Directory stores information about users as user properties, and Active Directory user properties can be looked up using the $adinfo function. This makes it possible, for example, to base a drive mapping on a user's home directory as stored in Active Directory.

To set this up, configure an environment variable that uses the function `$adinfo(homedirectory)` to set its value based on the user's home directory information in Active Directory; and then map the directory on the basis of this environment variable.

For example:

- At **Composition > Actions By Type > Environment Variables**, create an environment variable.
- Give it a name (for example, `HomeDrive`)
- In the **Value** field, enter: `$adinfo(HOMEDIRECTORY)`
- At **Composition > Actions By Type > Files and Folders > Drive and Port Mappings**, create a drive mapping
- In the **Share name** field, enter: `%HomeDrive%`

Result: when a user starts a session, the path stored in that user's Active Directory property **Home folder** is set as the value for the environment variable %HomeDrive%; and then the directory is mapped on the basis of this path as taken from the Active Directory.

7.4.2 Drive Substitutes

For some (legacy) applications it may still be necessary to use a fixed drive letter. You can substitute drives to create the drive needed. You can do this by using the **Drive Substitutes** option.

You can set the drive substitute to be dependent on **connection state**. For example, when working with a laptop, the mapping should only be set if the user is connected to the network. This means the required state must be on-line connection. If the mapping is not set to be connection state-dependent, it will be set permanently.

Configuring Drive Substitutes

- At **Composition > Actions By Type > Files and Folders > Drive Substitutes**, the option **Refresh Drive Substitutes when network connectivity changes** allows you to refresh Drive Substitutes automatically when the network connectivity of a session changes. This ensures that connection state-dependent Drive Substitutes become available or disappear correctly.
- You can override the global settings of this feature for specific Workspace Containers.
- When configuring a drive substitute, you can optionally enter a note in the **Administrative note** field. This is useful to differentiate the substitutes that you configured.
- When specifying the hide drives behavior for a drive substitute, the option **Always hide, but allow access** will hide drives, but they are still available to users that need access to them. This is useful, for example, for local floppy disks. If a local floppy disk is not hidden, this can seriously slow down the initial appearance of Windows Explorer or file dialog windows. You can change the default behavior for all drive substitutes if necessary.
- The field **Physical drive and path** specifies the physical drive and path to the drive that will be substituted for the virtual drive that you selected in the field **Virtual drive**.
- The **Required connection state** field specifies the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an online connection state.
- When a session starts, the applicable drive substitutes are set in the order in which they appear in this list. If necessary, change the order to ensure the correct processing.
- Click the **Access Control** tab to configure the Access Control criteria of the drive substitute.
- Click the **Workspace Control** tab to configure to which Workspace Container(s) the drive substitute applies.

7.4.3 Folder Redirection

At **Composition > Actions By Type > Files and Folders > Folder Redirection**, you can configure the redirection of Microsoft Windows User Shell Folders. Folder redirection enables the administrator to redirect the location of certain folders of the user profile to a different path, such as a shared network location. For example, the local folder `c:\Users\<username>\My Documents` can be redirected to a different **Target folder location** (e.g. `<networkshare>\Users\<username>\My Documents`). Up till now, folder redirection could only be done by creating a User Registry Setting or by defining a GPO. If the folder does not exist in the target location of the user session, it will be created automatically, if possible in the user context.

Some of the advantages of folder redirection are:

- user documents are available from any computer
- helps to reduce logon and logoff times (data is stored outside the user profile)
- reduces the risk of profile corruption
- increased security and availability of user data (safe storage and recovery on network location)

The following folders can be redirected:

Folder on Microsoft Windows Vista and higher	Folder on Microsoft Windows XP	Description
Appdata	Application Data	Default location for user application data and binaries (hidden folder)
Contacts	Not applicable*	Default location for users' Contacts
Desktop	Desktop	Desktop items, including files and shortcuts
Documents	My Documents	Default location for all user created documents
Downloads	Not applicable*	Default location to save all downloaded content
Favorites	Favorites	Internet Explorer Favorites
Links	Not applicable*	Contains Windows Explorer Favorite Links
Music	My Music	Default location for user’s music files
Pictures	My Pictures	Default location for user’s picture files
Saved Games	Not applicable*	Used for Saved Games
Searches	Not applicable*	Default location for saved searches
Start Menu	Start Menu	Default location for Start Menu
Videos	My Videos	Default location for user’s video files

* Microsoft Windows XP and before will not recognize these folder redirections.

Configuration of Redirections

- Shows the redirected folders, for example, `Favorites` may be redirected to `<networkshare>\Users\<username>\Favorites`. If several Folder Redirections have been configured, you can change the order in which the redirections will be carried out by clicking **Change order of execution** and using the arrow up and down icons.
- Select the **Windows folder** which must be redirected in the user session. See the table above for possible folders for redirection and the OS version to which they apply.
- Click  to select the **Target folder location** or enter the target folder manually. When entering the target folder manually, you should keep in mind that this applies to the user session environment. For example, a network location that the Administrator can access, can not necessarily be accessed by the user as well.
- If the folder does not exist in the target location of the user session, select **Create target if it does not exist** to create it automatically.
- The **Required connection state** field specifies the required connection state that allows folder redirection. For example, this allows you to configure folder redirection that will only take place if a computer is online. See Connection State Settings.
- Click the **Access Control** tab to configure the Access Control criteria of the Folder Redirection.
- Click the **Workspace Control** tab to configure to which Workspace Container(s) the Folder Redirection applies.

Configuration of Settings

- Shows whether Folder redirection has been enabled or disabled.
- You can override the global settings of this feature for specific Workspace Containers.

Notes

- With Folder Redirection, a backup is made of pre-existing folder redirections for that user and this backup is restored at the end of the user session. This is done because otherwise when, for example, a user is placed in a different Workspace Container, he/she could get invalid folder reference(s) due to Folder Redirection.
- When there are User Registry actions that are already configured, enabling Folder redirection will prompt a message that these actions may override Folder Redirections and need to be checked. For example, you may have a registry setting for the Folder Redirection for Citrix Servers, which applies to the Workspace Container Citrix Servers, which may conflict with other Folder Redirections. In this case, you have to be careful configuring a redirection for Citrix Servers in **Composition > Actions By Type > Files and Folders > Folder Redirection** as it will be overridden by the User Registry action.
- When using Folder Redirection, **User Profile Directory** Maintenance can no longer be used to manage the contents of these redirected folders, because they are no longer part of the user profile. When a folder is redirected to the user's home drive, you can use **User Home Directory** Maintenance to manage the contents of the folder.
- **Start Menu** will be redirected along with **AppData**, unless:
  - **Start Menu** itself has been configured for **Folder Redirection**
  - **Start Menu** has already been redirected by means of a GPO to a different path from **AppData** (also, for Microsoft Windows Vista and later, child shell folders of **AppData** will also be redirected)
- Any contents of the original **Start Menu** folder will NOT be copied to the redirected location.

Configuring folder redirection

Redirections tab

- Shows the redirected folders, for example, `Favorites` may be redirected to `C:\Users\%username%\Favorites`. If several Folder Redirections have been configured, you can change the order in which the redirections will be carried out by clicking **Change order of execution** and using the arrow up and down icons.
- You can override the global settings of this feature for specific Workspace Containers.
- Select the **Windows folder** which must be redirected in the user session. See the table above for possible folders for redirection and the OS version to which they apply.
- Click  to select the **Target folder location** or enter the target folder manually. When entering the target folder manually, you should keep in mind that this applies to the user session environment. For example, a drive mapping that exists in the Administrator's profile does not necessarily have to exist in the user's profile.
- If the folder does not exist in the target location of the user session, select **Create target if it does not exist** to create it automatically.
- The **Required connection state** field specifies the required connection state that allows folder redirection. For example, this allows you to configure folder redirection that will only take place if a computer is online. See Connection State Settings.
- Click the **Access Control** tab to configure the Access Control criteria of the Folder Redirection.
- Click the **Workspace Control** tab to configure to which Workspace Container(s) the Folder Redirection applies.
- With Folder Redirection, the original Windows Shell Folder settings are restored at the end of the user session. This is done because otherwise when, for example, a user is placed in a different Workspace Container, he/she could get invalid folder reference(s) due to Folder Redirection.

Settings tab

Shows whether Folder redirection has been enabled or disabled.

Examples

Folder Redirection versus User Profile Directory

These can be confusing as both can be used to manage user-dependent files. In most cases, a combination of Folder Redirection and User Profile Directory maintenance will be necessary. For example, an application or application plug-in may need some configuration settings from the local User Profile, but you want to store the user settings on a network drive at logoff for security reasons. Define the file containing the user settings as an object at **Composition > Actions By Type > Files and Folders > User Profile Directory**. Redirect the **AppData** folder to a network drive via **Composition > Actions By Type > Files and Folders > Folder redirection**. This way, the application can start up and the user settings are stored safely.

7.4.4 Folder Synchronization

Users often work from a variety of locations, and in each location they access, create, change and delete files and folders. This may lead to problems if users are unable to find the correct documents because they have different sets of documents, or different document versions, in different workspaces.

Use Folder Synchronization to solve this by synchronizing the files in two designated folders, in order to ensure that the correct set of files and folders is available in the user's workspace.

- Configure global Folder Synchronization actions to synchronize the contents of folders that should be up to date when a RES Workspace Manager session starts, ends, refreshes or reconnects or at specific intervals.
- Home folders are an example of folders that should be synchronized with a global Folder Synchronization action.
- Configure application Folder Synchronization actions to synchronize the contents of folders that should be up to date when a specific application starts or ends.

Folder Synchronization: global or application-based

- Configure global Folder Synchronization actions to synchronize the contents of folders that should be up to date when a RES Workspace Manager session starts, ends, refreshes, reconnects or at specific intervals. Home folders are an example of folders that should be synchronized with a global Folder Synchronization action.
- Configure application Folder Synchronization actions to synchronize the contents of folders that should be up to date when a specific application starts or ends.

Prerequisites

Microsoft .NET Framework 4.0 and Microsoft Sync Framework 2.1 must be installed on all Agents running user sessions in which folders are to be synchronized. Microsoft .NET Framework 4.0 must be installed separately; Microsoft Sync Framework 2.1 is automatically installed during installation of RES Workspace Manager. Both folders must be accessible in the user's workspace. For one-way synchronization, the user must have write permissions on the local folder. For two-way synchronization, the user must have write permissions on both folders.

Configuring folder synchronization

- On the **Properties** tab, you can choose to include or exclude read-only files, hidden files and system files. With two-way synchronization (Direction: **Both**), files deleted in one folder are also deleted in the other location. With single-direction synchronization **Direction: Upload**, files deleted locally will also be deleted from the remote location and with **Direction: Download**, files deleted from the remote location will also be deleted locally after synchronization.
- Optionally, on the **Filters** tab, you can filter a Folder Synchronization action to include only specific files (for example, `D-Energy.ppt`) or file types (for example `*.ppt`), and/or to exclude specific files, file types and folders.
- You can use the wildcard characters * and ? in the fields Files to include and Files to exclude.
- Separate multiple entries in the fields Files to include and Files to exclude with a semi-colon (;).
- You can specify folders that should be excluded by entering the location in the **Folder** field and clicking **Add**.
- To exclude a folder that is located in another folder, enter the full path. For example, if you only specify "temp", the folder "temp" in the root of the sync folder will be excluded; "temp" folders in other folders will not be excluded.
- The **Required connection state** field specifies the required connection state that allows synchronization. For example, this allows you to configure synchronization that will only take place if a computer is on-line.
- By default, files that are overwritten or deleted during the synchronization process are moved to the user's Recycle Bin, so that they remain available for recovery. This safety measure can be turned off if it is not necessary.
- Click the **Access Control** tab to configure the Access Control criteria of the Folder Synchronization.
- Click the **Workspace Control** tab to configure to which Workspace Container(s) the Folder Synchronization applies.

7.4.5 Directory Maintenance

The **Directory Maintenance** technology can be used for preparing and maintaining a user's home and profile directories.

Directory Maintenance is divided into a **User Home Directory** node and a **User Profile Directory** node. Both nodes allow you to configure a **model** or template of the files and folders that should be present on or copied to the user's home directory and/or the user's profile directory.

The User Home Directory and User Profile Directory nodes consist of two tabs:

- The **Files** tabs: these tabs allow you to configure the model directories of RES Workspace Manager. They provide an Explorer-like view of the model directories, files and subfolders. A model directory contains all folders and resources that you can use when configuring the contents of the user's home directory or profile directory.
- The **Actions** tabs: these tabs allow you to configure the contents of the user's home directory and profile directory, based on your selection of folders and resources from the model directories.

Configure Model Directories (Files tab)

- Click the **Files** tab of the **User Home Directory** or **User Profile Directory** node, depending on the directory that you want to configure.
- Select the folder to which you want to add a folder or resource and click **Add**. This will open the Select File(s)/Folder(s) window, which allows you to select and add folders and resources to the model directory.
- Select or browse to the file or folder that you want to add and click **OK**. The selected file or folder will be added to the **Model directory** folder of the **Home Directory** or **Profile Directory** node, depending on your selection in step 1. You can only use these files and folders to configure the user's Home Directory and Profile Directory.

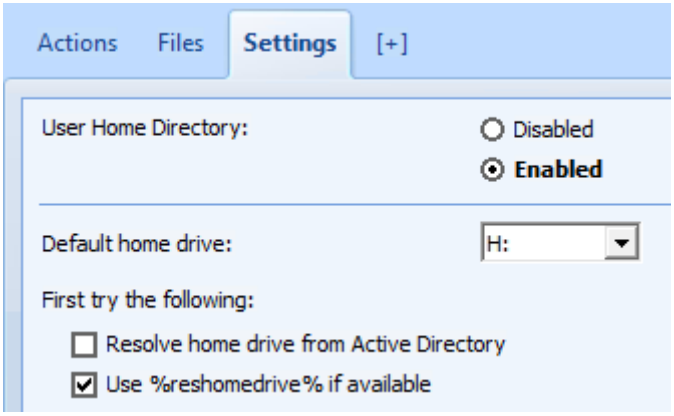
Configure Settings (Actions tab)

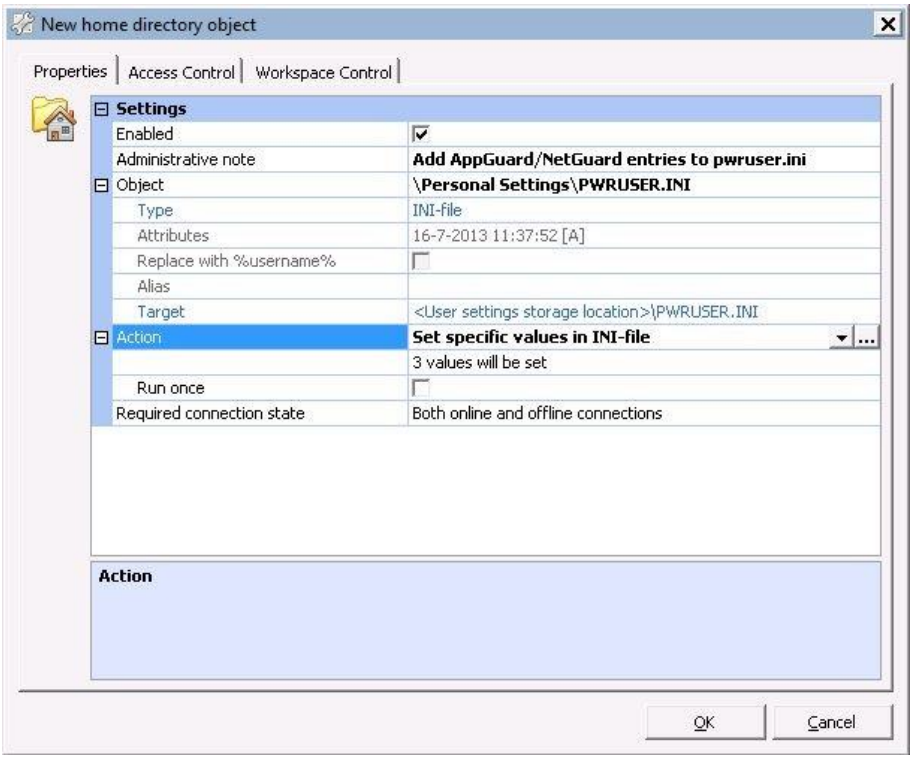
- When configuring the settings of a file or folder, you can replace its name with the user name. This is useful if you want to copy a file or folder with the same name as the user's logon name to the user's home directory.
- By specifying an alias for the object, the original object name will be overwritten when it is copied to the home directory of a user. This is useful if the home directory of a user should contain a specific object whose values depend on the group membership of the user.
- Select which action should be taken in the **Action** field, depending on whether you selected a folder or a file in the **Object** field. When specifying an Action for a file, the option **Set specific values in INI-file** allows you to configure INI file values. After configuring INI-file values, select **Run once** if these values should be set only once.
- **Required connection state** specifies the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an online connection state.

Specify the user's home directory drive (User Home Directory > Actions)

Select the drive in the **Drive to home directory** field at the **Home Directory Maintenance** node.

Select **Use %reshomedrive% if available** to create exceptions to the default Drive to home directory setting by using the `%reshomedrive%` environment variable.





The Overview in the users Workspace Analysis Details also shows the Home Directory and Profile Directory rules that apply to the user. See **Workspace Analysis** (on page 241).

Note

- All actions taken in the **Home Directory** node will be logged, which allows you or a technical manager to evaluate in detail which files and/or directories have been copied to a specific user's home directory.
- **Diagnostics > Event Log** in the **Workspace Analysis** window displays the Home Directory and Profile Directory rules that apply for the user.
- You can use environment variables (e.g. "`%username%`")

7.4.6 Printers

Depending on the physical location of the desktop or laptop, different printers should be available to the user. You can use **Composition > Actions By Type > Printers** to achieve this.

You can set a printer as the **default** printer for the selected type of access control. It is also possible to define a **backup** printer for process-critical printing situations. To do this, enable the **Failover** option.

The RES Workspace Manager Workspace Composer shows a simple list of available printers, and so helps the user to select a default printer or open a Print Status window. The user can even set a default printer based on his work location. You can also allow the user to connect to additional printers.

Configuring printers

- If you select **Force mandatory default printer (reset default printer during each logon)**, the advanced options in the user's "Printing Preferences" will be disabled. Although the end user will be able to set a different printer as default within a session, the centrally configured default printer will be reset at the start of each new session.
- **Also connect default / all printer(s) using VDX plugin** also connects printers from the remote session in your local desktop. This allows, for instance to use a printer from your virtual desktop on your local desktop or in an application that is configured as a workspace extension (i.e. that runs from your local desktop). If **Connect default printer using VDX plugin** is enabled, the default printer of your virtual desktop will be used as default printer in your workspace extensions. If this option is not selected, the default printer of your local desktop will be used.

Disconnect network printers:

- **Before logging off**, RES Workspace Manager will clean the user profile from user-connected and disabled printers. If you clear the check box **Disconnect network printers before logging off**, these settings will be preserved in the user's profile.
- **Before logging on or on reconnect**, RES Workspace Manager will clean the user profile from user-connected and disabled printers. If you clear the check box **Disconnect network printers before logging on or on reconnect**, these settings will be preserved in the user's profile.
- **Skip unmanaged printers**: Within RES Workspace Manager, an unmanaged printers is a printer that does not have a managed equivalent in an RES Workspace Manager session. If both a managed and an unmanaged version of a printer exist, the unmanaged version will be replaced by a managed version after logging on. When this option is enabled, only network printers that are managed by RES Workspace Manager will be disconnected before logon/logoff, all other printers will not be touched. The advantage of keeping unmanaged printers is, for instance, when you have defined an unmanaged printer you only use at home, you do not have to reconnect this printer each time you need it.

Refresh printers:

- **On reconnect** causes RES Workspace Manager to reprocess all Network Printers, to determine which printers should be connected when a previously disconnected terminal session is reconnected.
- **On session refresh** causes RES Workspace Manager to reprocess all Network Printers, to determine which printers should be connected when a user session refreshes.
- **When network connectivity changes** helps workstations and laptops to automatically reconnect printers when switching from offline network connection to online. To work properly, the checkbox **Do not refresh Workspace when network connectivity changes** at **Composition > Desktop > Lockdown and Behavior** must be unchecked.
- When configuring a network printer, optionally enter a note in the **Administrative note** field. This is useful to differentiate the Printers that you configured.
- **Fast connect** allows users to start their sessions faster. The **Fast Connect** option is not available for Printers that are configured for an application.
- When selecting the option **Fast connect**, the option **Wait for task to finish before continuing** becomes unavailable, because driver checks and permission checks will first be performed when the user actually connects to the printer.
- When clearing the option **Wait for task to finish before continuing** the option **Fast connect** becomes unavailable, because the task will be performed asynchronously.
- When specifying whether printing preferences should be preserved, if you select **Default**, the default settings as configured in the node **Composition > User Settings** will be applied. If you select **Never save** or **Always save**, this will overrule the default settings as configured in the **User Settings** node. The option **Set as default printer** for Printers is mandatory when configuring a printer for an application, but this will not reset the user's preference. The next time the user logs on, the preferred default printer will be restored. The user will also be notified of this event by the "Printing preferences" tool.
- The option **Failover** allows you to configure a backup printer that the user can connect to if it is not possible to connect to the primary printer, for example because the specified printer driver is unknown or if the printer server is unavailable.
- The **Required connection state** field specifies the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an on-line connection state.
- Click the **Access Control** tab to configure the Access Control criteria of the Printer.
- Click the **Workspace Control** tab to configure to which Workspace Container(s) the Printer applies.
- When a session starts, the applicable printers are set in the order in which they appear in this list. If necessary, change the order to ensure the correct processing.

Tip

Sometimes the message "Composing default printer" appears in the Startup screen, although a default printer was defined. This is caused by the fact that the workstation cannot access the printer due to missing user credentials. In RES Workspace Manager user credentials cannot be defined for printers. A possible workaround is to define a drive mapping to the same network location (or subdirectory) with the proper user credentials. Any driveletter can be assigned. This will speed up the connection to the printer considerably.

Using Locations and Devices for Printers

Because printers are usually used per location, you can use **Zones** / **Workspace Containers** to set up printers. By creating Zones / Workspace Containers you can set up printers per location. It has the advantage that for instance mobile users will automatically connect to the right printer when using a mobile computer at different locations.

Configure Zones for different IP ranges if your users use roaming workplaces or when multiple branches of your company share the same print server.

7.4.7 User Registry

With the **User Registry** technology it is possible is to set up registry keys and policies for (groups of) users, based on their specific situations and needs. For example, it is possible to set registry settings based on the selection of the user's RES Workspace Manager language.

Registry keys (HKCU) can be imported and exported, which facilitates entering or changing registry keys. If you select the **Run once** option when implementing a registry setting, it will only be applied the first time a user logs on.

Documentation on registry keys can be found at various locations. Registry keys changing Windows settings can be found in the Windows Resource Kit. Documentation on application registry settings may be harder to find, since not all applications provide documentation regarding registry settings. Contact the application vendor for more information.

Policies

User Registry also supports Windows policy files (`.adm`) in the registry section. When adding a new policy template, first select a policy file to base the template on.

Configuring Registry Settings

Configuration

1. Click **New Registry**, this will open the **New registry settings** window.
2. Click the **Properties** tab.
   a) Enter the name of the registry setting in the **Name** field.
   b) Optionally enter a note in the **Administrative note** field. This is useful to differentiate the registry settings that you configured.
   c) To enable the registry setting, select **Enabled**.
   d) Select **Run once** to limit implementation of the registry setting to a user's first startup.
   e) Select **Ignore registry redirection (on 64-bit operating systems)** to map the registry value (new or modified) to the path specified by the user. If this option is not selected, the registry value may be mapped to a location under Wow6432Node on a 64-bit operating system.
   f) In the **Required connection state** field, select the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an online connection state. See Connection State Settings.
   g) Right-click **HKEY_CURRENT_USER** and select an action from the **Registry** section. The first five actions are explained based on an example where **HKEY_CURRENT_USER** is the subtree, **SOFTWARE** is the key and **RES** is the subkey (**HKEY_CURRENT_USER\SOFTWARE\RES**).

How to add a registry subkey

1. Right-click **HKEY_CURRENT_USER**.
2. Click **Open HKEY_CURRENT_USER**. This will open the **Pick keys/values from registry** window.
3. Expand **HKEY_CURRENT_USER** and **SOFTWARE**.
4. Select **RES** and click **New**.
5. Click **Close** to close the **Pick keys/values from registry** window.

How to add a new subkey to an existing subkey

1. In the **New registry setting** window, expand **HKEY_CURRENT_USER** and **SOFTWARE**.
2. Right-click the **RES** subkey.
3. Point to **New** and click **Key**.
4. Enter **TestSubkey** in the folder that is added and press ENTER.

How to add or change a registry subkey value

How to add a new string value

1. In the **New registry setting** window, expand **HKEY_CURRENT_USER**, **SOFTWARE** and **RES**.
2. Right-click the **TestSubkey** subkey.
3. Point to **New** and click **String Value**.
4. Enter **TestString** and press ENTER.

How to edit the value of a subkey

1. Right-click the value that you just added.
2. Click **Modify**. This opens the **Edit String** window.
3. Enter **1** in the **Value data** field.
4. Enter "This is a test value" in the **Administrative Note** field. This field can be used to describe the function of the registry value. If you create an Instant Report of the registry setting, any annotations will be included.
5. Click **OK**.

You can add the following registry subkey values:

Value	Function
String Value	Adds a string value. Most information about hardware components is stored as binary data and shown in hexadecimal format.
Expandable String Value	Adds a variable-length string value. This data type includes variables that will be resolved when an application or service uses the data.
Multiple String Value	Adds a multiple string value. In general, this type is used for values that contain lists or multiple values in a form. Separate multiple values with spaces, commas or other marks.
Binary Value	Adds a binary value. This data type is generated by hardware device drivers and the physical devices it controls. It is shown in hexadecimal format as a binary value.
DWORD Value	Adds a DWORD value. This data type is a number of 4 bytes long (32-bit integer). Many parameters for device drivers and services are this type and are shown in binary, hexadecimal or decimal format.

How to rename a registry subkey or value

1. Expand **HKEY_CURRENT_USER**, **SOFTWARE** and **RES**.
2. Right-click the **TestSubkey** key.
3. Click **Rename**.
4. Enter **RESTest** and press ENTER.

How to convert a registry value to a registry value of a different type

1. In the **New registry setting** window, right-click the **TestSubkey** subkey.
2. Point to **Convert to** and click **Expandable String Value**. This will convert the TestSubkey from a string value to an expandable string value. You can only convert string values, expandable string values and multiple string values to values of these types.

How to remove a registry subkey or value

How to remove the value from a subkey in the registry

1. Expand **HKEY_CURRENT_USER**, **SOFTWARE** and **RES**.
2. Select the **RESTest** subkey.
3. Right-click the **TestString** value and click **Toggle "remove this value"**. This will remove the value from the registry subkey in the registry.

How to remove a subkey from the registry

1. Expand **HKEY_CURRENT_USER**, **SOFTWARE** and **RES**.
2. Right-click the **RESTest** subkey and click **Toggle "remove this value"**. This will remove the registry subkey and its underlying values from the registry.

How to delete a subkey

1. Expand **HKEY_CURRENT_USER**, **SOFTWARE** and **RES**.
2. Select the **RESTest** subkey.
3. Right-click the **TestString** value and click **Delete**.
4. Click **Yes** to confirm that you want to delete the value.

Registry Tracing

When you make changes to the preferences of an application, these are usually stored as a registry setting in HKEY_CURRENT_USER. If you want to add these registry settings to **Composition > Actions By Type > User Registry** manually, you need to know the exact location of these settings in the registry. With the functionality Trace registry changes (available from the Action menu when adding a new User Registry setting), this is not necessary. When tracing the registry changes that are made by an application's process, you can choose the relevant registry setting(s) from a list of logged registry changes and convert them to a User Registry setting. This makes it easier to add registry settings.

You can use registry tracing to configure global User Registry settings, as well as User Registry settings that are set when a user starts an application.

To use Trace registry changes:

- Add or edit a User Registry item (in an application's Configuration section on the Action tab, or at **Composition > Actions By type > User Registry**).
- Go to **Action > Registry > Trace registry changes**.
- In the **Trace registry changes** window, the **Process** field shows the application's command line. You can change this if necessary, either by typing a process yourself, or by selecting a process that is currently running.
- For processes traced from an application's **Configuration** section on the **Action** tab, the button **Run now** opens the application with the full RES Workspace Manager configuration, including settings, etc. For example, if a command is configured as a setting for the application, then this command will also be executed if you start the application with the **Run now** button in the **Trace registry changes** window.
- For processes traced from **Composition > Actions By Type > User Registry**, the **Run now** button starts the selected process as if from the command prompt.
- After clicking **Start trace**, you can go to the application and make the changes to the preferences you wish to store. The **Trace registry changes** window will reflect all the registry changes made by the application.
- Click **Stop trace** when you have changed all the settings you needed to change. Select the check boxes of the changes that you want to set as a User Registry and click **Add**.

How to import and export registry keys

How to import registry files

1. Select the folder in which you want to import or export registry files and click **Registry** in the menu bar.
2. Click **Import registry file**. This will open the **Import Registry File** window.
3. Select the registry file and click **Open**. This will open the **Import registry file** window.
4. Select one of the merge options:

Item	Function
Replace existing data	Replaces the existing registry file with the imported registry file.
Perform incremental merge with existing data	Adds the data in the imported registry file to those in the existing registry file.
Perform differential merge with existing data	Replaces only those data in the existing registry file that differs from the imported registry file.

How to export registry files

1. Select the registry file that you want to export and click **Registry** in the menu bar.
2. Click **Export registry file**. This will open the **Export Registry File** window.
3. Select the location, enter a name for the file and click **Save**.

Toggle Remove

In RES Workspace Manager it is also possible to remove specific registry keys and/or values from a user profile, each time User Registry is executed. To achieve this, create a User Registry object that contains the keys and values that should be deleted from the user profile:

- Select the registry key or value you want to delete.
- Right-click the specific key or value.
- Select **Toggle - remove this key and subkeys** or select **Toggle - remove this value**.

Language Identity

It is also possible to link a registry key setting to a **language** setting, allowing an application to start in the user's preferred language (which can be selected on the **Options** tab of the "Workspace Preferences" tool). This functionality is beneficial for multilingual businesses. However, the application must be able to change a language setting using a registry setting.

Configuring registry policies

When you select a policy file, its contents will be displayed and you can set new policies. If a policy requires additional data, a detailed policy window is displayed in which you can type data. When typing textual data in this window, it is possible to use variables such as "`%username%`" or "`%homedrive%`".

You can specify the order in which registry files and policies should be processed with the **Change order of execution** option.

When policies have been set (switched on or off), the menu item **View resulting registry** in the **Policy** window enables you to view the registry keys and values that result from the policies. It is also possible to export these keys and values to a registry file for later use.

The policy template will be copied to the Datastore, which allows it to be used at all times and on all servers.

1. Click **New Policy**, this will open the **Select ADM file** window.
2. Select the policy file on which the template will be based. You can select ADM files and ADMX files, which are xml-based.
   - Alternatively, click **Add** or **Remove** to add or remove ADM(X) files.
3. Click **OK**. This will open the **New registry setting (based on <adm file>)** window.
4. Click the **Properties** tab.
   a) Enter the name of the registry setting in the **Name** field.
   b) Optionally enter a note in the **Administrative note** field.
   c) To enable the registry setting, select **Enabled**.
   d) Select **Run once** to limit implementation of the registry setting to a user's first startup.
   e) Expand the contents of the ADM file.
   f) Double-click a setting to view its details or right-click the setting and click **Explanation** to view an explanation of the setting.
5. Click the **Access Control** tab to configure the Access Control criteria of the registry setting.

Click the **Workspace Control** tab to configure to which Workspace Container(s) the registry setting applies.

7.4.8 Execute Command

At the **Execute Command** section you can start external non-RES Workspace Manager tasks or applications when a user logs on or off.

This can be anything from an enterprise-wide questionnaire application to a simple cleanup task.

Configuring commands

- When configuring a command, the option **Run Hidden** runs the command hidden from the user.
- RES Workspace Manager can detect whether the command has run before for that user, on that computer, or for the combination of that user on that computer. In the **Run once** field, you can configure whether the command should be executed or skipped depending on this information:
- Select **Run once** to execute the command only if it has not yet been executed for the user starting the session.
- Clear **Run once** to execute the command regardless of whether it has been executed before.
- If you need to repeat an **existing** command that has been configured to **Run once**, select **Clear history**. If you select **Clear history**, the history of the command will be cleared and the command will be repeated once.
- If a command has been configured to run at logoff, the option **Wait for task to finish before continuing** will always be selected. Specify a timeout in seconds to ensure RES Workspace Manager does not wait if the task is unable to finish.
- **Required connection state** specifies the required connection state that allows the command to be executed. For example, this allows you to configure a command that only synchronizes user files between a laptop and the network if the laptop has an online connection state. See Connection State Settings.
- For App-V applications, the option **Run outside App-V virtual environment** is available. This allows the command that was configured for the application to run outside the App-V bubble of that application.
- On the **Script** tab you can directly enter script contents. Enter (only) `%script%` in the command line on the **Properties** tab, to refer to the script tab content. Note that the correct **file extension of the script** is entered on the **Script** tab.
- It is not possible to execute a Visual Basic- or PowerShell-script in combination with only the `%script%` variable in the command line. In that case, use the following in the command line:
  - To execute Visual Basic-scripts use `cscript.exe %script%`.
  - To execute PowerShell-scripts use `PowerShell.exe %script%`.
- Click the **Access Control** tab to configure the Access Control criteria of the command.
- Click the **Workspace Control** tab to configure to which Workspace Container(s) the command applies.

Note

The option **Execute Command** can be **Run using Dynamic Privileges**. This means that the task will run "elevated", using Administrative Privileges, while maintaining default privileges for the user. The option **Run using Dynamic Privileges** is part of the functionality of the Adaptive Security module and therefore is only available if this module is included in your license. For full details, please refer to the RES Workspace Manager Module Comparison Chart available at http://www.ressoftware.com/workspace-manager-editions.

7.4.9 Microsoft System Center Configuration Manager Software Distributions

At **Composition > Actions By Type > Microsoft ConfigMgr**, you can view and configure Microsoft System Center Configuration Manager software distributions. This allows you to deploy software distribution Programs in the user workspace.

You can only configure Microsoft Configuration Manager software distributions if you have enabled **Microsoft System Center** in the **Setup** menu and are connected to a Microsoft System Center Configuration Management Server.

Software distribution Configuration

To add a software distribution that should run when a session starts, go to **Composition > Actions By Type > Microsoft ConfigMgr**. See RES Workspace Manager Help for configuration settings.

- You can override the global settings of this feature for specific Workspace Containers.

Configuring software distributions for Applications

To add a software distribution that should run when an application starts, open the application at **Composition > Applications** and go to **Configuration > Actions**. Configuring these software distributions is the same as on global level.

- If the **Wait for action to finish before continuing** has been enabled for a software distribution on an application, a notification is displayed in the user session if a user starts the application and the Package is deployed. This notification window allows the user to select **Dismiss and notify me when done** which allows the user to continue working with already available applications while the Package is deployed.

Note

You can easily move Actions from one application to another; from an application to global; and from global to a specific application. To do so, right-click one or more selected Actions and choose **Move**.

7.4.10 LANDesk

At **Composition > Actions By Type > LANDesk**, you can view and configure LANDesk software distributions. This allows you to deploy software in the user workspace.

You can only configure LANDesk software distributions if you have enabled **LANDesk** in the **Setup** menu and are connected to a MBSDK Web Service.

Software distribution Configuration

To add a software distribution that should run when a session starts, go to **Composition > Actions By Type > LANDesk**. See RES Workspace Manager Help for configuration settings.

- You can override the global settings of this feature for specific Workspace Containers.

Configuring software distributions for Applications

To add a software distribution that should run when an application starts, open the application at **Composition > Applications** and go to **Configuration > Actions**. Configuring these software distributions is the same as on global level.

- If the **Wait for action to finish before continuing** has been enabled for a software distribution on an application, a notification is displayed in the user session if a user starts the application and the Package is deployed. This notification window allows the user to select **Dismiss and notify me when done** which allows the user to continue working with already available applications while the Package is deployed.

Note

You can easily move Actions from one application to another; from an application to global; and from global to a specific application. To do so, right-click one or more selected Actions and choose **Move**.

7.4.11 Automation Tasks

Automation Tasks allow you to run specific RES Automation Manager Tasks in the user workspace, such as the installation of software or the creation of user profiles. RES Workspace Manager will run these Tasks during the logon process of a user.

You can only configure RES Automation Manager Tasks if you have enabled **RES Automation Manager Integration** at **Setup > Integration > RES Software > RES Automation Manager** and are connected to a RES Automation Manager Datastore.

Configuring Automation Tasks

- To configure an Automation Task that should run when a session starts, go to **Composition > Actions By Type > Automation Tasks**.
- To configure an Automation Task that should run when an application starts, open the application at **Composition > Applications** and go to **Configuration > Actions**.
- You can override the global settings of this feature for specific Workspace Containers.
- When configuring an Automation Task, optionally enter a note in the **Administrative note** field. This is useful to differentiate the Automation Tasks that you configured.
- Click  in the **Task** field to load the available RES Automation Manager Projects and Modules from the RES Automation Manager environment that you specified at **Setup > Integration > RES Software > RES Automation Manager**. This allows you to select the RES Automation Manager Projects or Modules that should be part of the RES Automation Manager Task.
- **Skip if application executable was found** (only available on application level) when selected, a check will be done whether the application executable is present on the client computer before the task is executed. When the option is not selected, the task is executed as configured when the application is started.
- RES Workspace Manager can detect whether the Automation Task has run before for that user, on that computer, or for the combination of that user on that computer. In the **Run once** field, you can configure whether the Task should be executed or skipped when a user starts the application:
- **No**: the Automation Task will be executed, irrespective of whether it has been executed before.
- **Per user**: the Automation Task will be executed once for each user who logs on to the RES Workspace Manager environment.
- **Per computer**: the Automation Task will be executed once for each computer in to the RES Workspace Manager environment.
- **Per user per computer**: the Automation Task will be executed once for each user who logs on to the RES Workspace Manager environment on a specific computer.
- If you need to repeat an **existing** Automation Task that has been configured to **Run once**, select **Clear history**. This resets the count, so that the existing Automation Task is executed again throughout the environment, according to the rules selected for **Run once**.
- When you configure a custom message, you can communicate additional information about the Automation Task to the user.
- **Wait for task to finish before continuing** forces RES Workspace Manager to finish the task before continuing with the next Task. Clear this check box to force RES Workspace Manager to continue with the next Task if the Task does not complete. It can be useful to select this option when you have configured a custom message: this allows the user some additional time to read this message. However, if the Automation Task has not started before the specified timeout expires, the Task will be canceled.

- **Run before other actions** makes it possible to specify that the Automation Task should be executed before other configuration Actions (except Environment Variable Actions). At application level, an Automation Task that is configured to **Run before other actions** will appear on top of the list of Actions on the **Actions** tab; The option **Run before other actions** will automatically be selected or cleared again when moving an Automation Task in the list by using the arrows.
- **Required connection state** specifies the required connection state that allows the Task to be executed. For example, this allows you to configure a Task that only runs if the laptop has an online connection state.
- Click the **Parameters** tab to view which parameters will be used in the Automation Task. This tab is only available if the selected RES Automation Manager Project or Module contains parameters.
- Click the **Access Control** tab to configure the Access Control criteria of the Automation Task.
- Click the **Workspace Control** tab to configure to which Workspace Container(s) the Automation Task applies.

7.4.12 Environment Variables

Environment Variables are variables set in the memory of the user's workstation or session.

These variables are often used by applications, for example to determine who a user is and what his default path structures are; or what the system date and time is. The option Environment Variables enables you to set or modify environment variables based on various types of access control.

Windows provides several useful variables, such as user name and computer name. You can use these variables in your values by using the percentage character (for example `%username%` and `%computername%`).

You can modify the order of execution by setting an order number in the order column. You can change the order by selecting the option **Change order of execution**.

Configuring Environment Variables

- To configure an Environment Variable that should be set when a session starts, go to **Composition > Actions By Type > Environment Variables**.
- To configure an Environment Variable that should be set when an application starts, open the application at **Applications** and go to **Configuration > Actions**.
- At **Composition > Actions By Type > Environment Variables**, the option **Reset Environment Variables on refresh of workspace** allows you to reset Environment Variables on a refresh of the user workspace. This ensures that connection state-dependent Environment Variables are resolved correctly.
- You can override the global settings of this feature for specific Workspace Containers.
- When configuring an Environment Variable, optionally enter a note in the **Administrative note** field. This is useful to differentiate the variables that you configured.
- In the **Value** field, you can use Microsoft Windows environment variables and the functions `$adinfo(<property>)`, `$usershellfolder(<folder>)`, `$substring`, `$endstring`, `$lowercase`, `$uppercase` and `$autocount`.
- When a session starts, the applicable Environment Variables are set in the order in which they appear in this list. If necessary, change the order to ensure the correct processing.
- The **Required connection state** field specifies the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an online connection state.
- Click the **Access Control** tab to configure the Access Control criteria of the environment variable.
- Click the **Workspace Control** tab to configure to which Workspace Container(s) the environment variable applies.

Example

You can use the **%deskpic%** variable to display a custom desktop picture for a specific (group of) user(s). The variable contains the file name of the picture to be displayed on the desktop, which must exist as desktop image resources. When RES Workspace Manager is started, this variable applies to each user that is member of the Non-management group, and places the **Non_mgmnt_back.bmp** picture on his desktop.

7.4.13 Linked Actions

When configuring Actions for applications it is possible to add **Linked Actions**. When adding a linked action the only configuration to be made is selecting the source application, containing the actions to be used.

This allows, for example, creating an application with a default set of Actions and linking various other applications to that source application, thereby making it unnecessary to create multiple applications and creating the same set of Actions for each application.

Configuring linked actions

Linked Actions - It is possible to implement the Actions configured for another application. When adding a linked action the only configuration to be made is selecting the source application, containing the actions to be used.

Linked Actions Restrictions

- Execution of "Linked Actions" is restricted based on:
- The Access Control set on the **Actions** configured for the source Managed Application
- The Workspace Control set on the **Actions** configured for the source Managed Application.
- Access Control configured for the source Managed Application is ignored.
- Workspace Control configured for the source Managed Application is ignored.
- Actions with the setting "Run Once" should only run once for each user, even if several applications reference the same Action.

Linked Actions Relationships

- Managed applications are allowed to link to multiple managed source applications.
- Multiple managed Applications (targets) are allowed to link to a single managed source application.
- Linked Actions are not allowed to link to any managed application which itself has "Linked Actions" Actions to another managed application.
- Managed Applications are not allowed to link to the same managed source application more than once.

7.5 Desktop

You can configure settings options concerning the appearance and the lockdown of the end user's workspace in the RES Workspace Manager Console at **Composition > Desktop**.

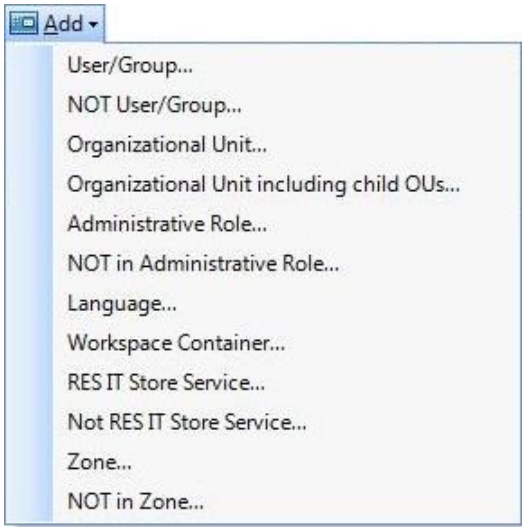
These settings include:

- Shell
- Background
- Lockdown and behavior
- Screensaver

7.5.1 Shell

At **Composition > Desktop > Shell**, you can define which shell should be used: the **RES Workspace Manager shell** or the (RES Workspace Manager-managed) **Microsoft Windows shell**. This is the shell the users are presented with in their workspace.

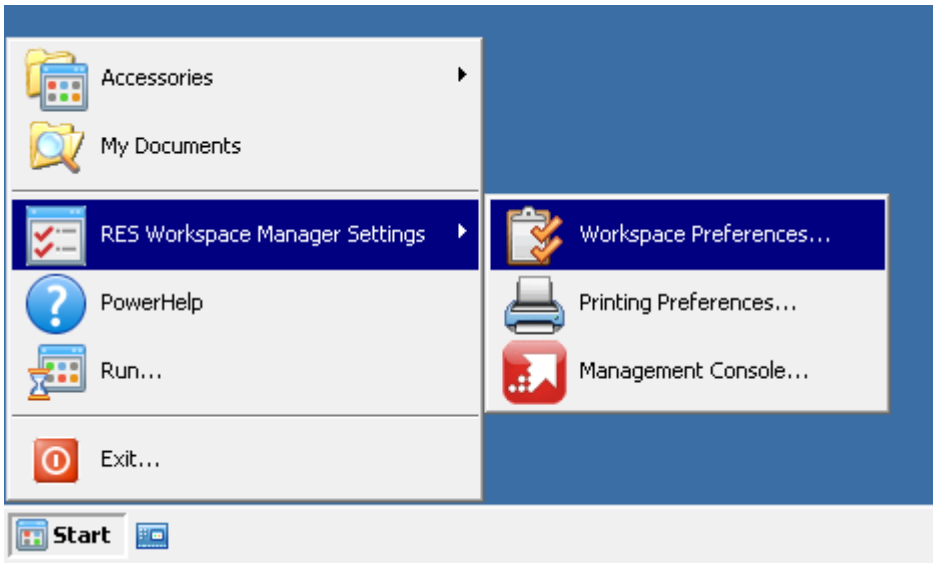
Here you can also exclude specific OUs, Groups, Users, Administrative Roles, Languages, Workspace Containers, Zones, or RES IT Store Services from the default shell. You can select Users and Groups from multiple domains, if configured.



A few of the benefits of the **RES Workspace Manager shell** are:

- Users do not have to attend a course every time Microsoft releases a new version of Windows.
- One company look and feel, regardless of the Windows version used.
- It provides additional menu- and application-related information for the users.

- Upgrading to a new Windows version poses no stress for users and administrators.



Notes

- When a user switches from the RES Workspace Manager Shell to the Microsoft Windows Shell, all configured settings will be remembered by both shells. When the RES Workspace Manager session ends and the Microsoft Windows Shell was used, all original settings will be restored in the profile of the user.
- The RES Workspace Manager shell has some extra configurable options (e.g. the information screen).
- The Windows shell makes use of `explorer.exe` which **might** be needed by some applications, but is less uniform (e.g. it allows the usage of themes).
- In the Microsoft Windows Shell, dragging and dropping items on the desktop or in the QuickLaunch area will be detected by the "Workspace Preferences" tool. This enables coexistence of both RES Workspace Manager shortcuts and document shortcuts. Users can customize their shortcuts in the Taskbar Settings window or with the "Workspace Preferences" tool.

7.5.2 Background

At **Composition > Desktop**, in the background section you can:

- select a picture (for example, your company logo) as well as the placement of that picture.
- use a variable desktop picture.

Select the option **Use %deskpic% variable** to define a variable desktop picture. You can do this at **Composition > Actions By Type > Environment Variables**. Here you can configure what pictures need to be used for what groups (OUs, NT etc.). The picture that is used with the variable is stored in the resources and is therefore always available. See Environment Variables for more information.

- In the **Default desktop colors** section you can select a default background and text color for your environment.
- Click the **Preview** button to view a preview of the selected settings.

Note

Make sure all files are available as desktop picture resources. By clicking the **Picture** button you can add a picture to the desktop picture resources. Both BMP and JPG pictures are supported for the desktop.

7.5.3 Lockdown and Behavior

Once the appearance of the Desktop has been set, you can hide/disable/remove specific settings in order to secure it fully.

Lockdown options can be set related to:

- **Workspace Composer**: hide/disable/remove options related to the Workspace Composer (irrespective of the shell used).
- **Start Menu and Taskbar**: hide/disable/remove specific Start Menu and Taskbar options from either the Windows shell, the RES Workspace Manager shell or both shells.
- **Personalizaton by end user**: hide/limit specific options in Printing Preferences and Workspace Preferences.
- **Windows Explorer**: hide/disable/remove specific options from the Windows Explorer application.
- **Microsoft Windows Shell**: hide/disable/remove specific options from the Windows Operating System.
- **RES Workspace Manager Shell**: determine specific behavior for the RES Workspace Manager Shell.

Optionally you can enter (part of) a keyword in the **Instant Search** field to find the setting you need.

Certain options in **Lockdown and Behavior** are always evaluated by RES Workspace Manager, even if **Lockdown and Behavior** is **Disabled**.

- Options marked with  are always evaluated and, if selected, applied.
- Options marked with  are only evaluated if **Lockdown and Behavior** is enabled. If **Lockdown and Behavior** is disabled, these options are grayed out.

Note

For a specific explanation of the available settings, see the RES Workspace Manager Help which is available from the Console by pressing F1.

7.5.4 Screensaver

At **Composition > Desktop > Screensaver**, you can set:

- A screensaver background image
- A variable screensaver picture.

Select the option **Use %saverpic% variable** to define via the RES Workspace Manager environmental variable `%saverpic%` what pictures need to be used for what groups (OUs, NT etc.). See Environment Variables for more information.

Notes

- The Microsoft Shell only supports BMP images for the screensaver. The RES Workspace Manager Shell supports BMP and other formats.
- Make sure all bitmaps are available as screensaver image resources. By clicking the "Image" button you can add a picture to the screensaver image resources.

When a mandatory timeout for the screensaver is set, the user can no longer set this time in his "Workspace Preferences" tool.

7.6 User Settings

RES Workspace Manager has a method of preserving and applying user settings independent from the Windows profile called **Zero Profile Technology**. Zero Profile Technology automatically detects user settings that are being changed by the user. These settings are preserved immediately outside the profile. When these settings are required by the Windows desktop or application, they are applied just in time.

The following assigned profile types are supported:

- Local profiles (version 1, 2)
- Roaming profiles (version 1, 2)
- Mandatory profiles (version 1, 2)

The profiles version 2 are used by Microsoft Windows Vista, Microsoft Windows Server 2008 and higher.

For more information about User Profiles, please see Microsoft references:

- Microsoft Technet | User Profiles (http://technet.microsoft.com/en-us/library/cc737881(WS.10).aspx)
- Managing User Profiles (http://technet.microsoft.com/en-us/library/bb726990.aspx)
- How to create and Assign User Profiles for Users in a Domain (http://support.microsoft.com/kb/128624)
- Managing Roaming User Data Deployment Guide, scenario 3 (http://download.microsoft.com/download/3/b/a/3ba6d659-6e39-4cd7-b3a2-9c96482f5353/managing%20roaming%20user%20data%20deployment%20guide.doc)

Users can change certain settings in a session, such as their default printer, their mouse orientation, and the view in which an application should open. Applications and processes store such user settings in keys and values in the user-specific part of the registry (HKEY_CURRENT_USER), and in configuration files in the user's profile directory.

However, user profile directories and HKEY_CURRENT_USER are not always preserved when the user logs off. This is particularly the case if you use mandatory profiles, or if you use roaming profiles in combination with passthrough applications in a Citrix XenApp environment.

With RES Workspace Manager Zero Profile Technology, you can preserve changes that users make to certain settings, files and folders during a session. These User Settings are preserved in a network location or at a local cache location outside the user profile and are restored automatically when the user logs on again. This is achieved independent of the user's profile.

7.6.1 Zero Profile Modes

- **Capture targeted items on application/session end** - Preserves specified parts of HKEY_CURRENT_USER and of the user profile directory when the session ends or when the user closes an application.
- **Track any changed setting within scope immediately (global)** - Automatically tracks specific trees in HKEY_CURRENT_USER and/or the user profile directory tree and immediately preserves any changes that occur there.
- **Track any setting changed by application immediately (application)** - Automatically tracks and immediately preserves all changes made by a specific application. This mode preserves all changes that the application's process makes in the registry at HKEY_CURRENT_USER and to files and folders in the user's %appdata% folder. This option is not available for Citrix Streamed Applications.
- **Capture targeted items once, then track further changes** - If this mode is selected User Settings will run once with the Zero Profile mode set to **Capture targeted items on application/session start/end**. The second time the Managed Application is run or the second time a session is started User Settings will run in the Zero Profile mode **Track any setting changed within scope/by application immediately**. By using this option it becomes very easy to use User Settings to migrate personal settings from one machine to another: With the **Capture targeted items once, then track further changes** mode it is easy to transfer all stored changes that were made on system A and track all new changes on system B with **Track any setting changed within scope/by application immediately**. Note that you need to specify Targeted items and possibly Excluded items.

Capture targeted items on application/session end

Use the Zero Profile modes **Capture targeted items on application/session end** (application) and **Capture targeted items on session end** (global) to preserve a list of specific items, as configured on the **Capturing** tab. Predefined Templates are available for a select number of applications and Control Panel options. You can use User Settings templates for the following applications:

User Settings templates available for applications listed below		
Windows	▪ Control Panel	General ▪ Accessibility Options, Desktop Content, Desktop Icons, Keyboard Settings, Mouse Settings, Regional and Language options, All Control Panel Settings Vista or later only ▪ Desktop Gadgets, Screen Saver, Sounds, Start Menu, Taskbar, Visual Settings, Toolbars Windows 7 only ▪ Themes XP and 2003 only ▪ Internet Options XP only ▪ Display

User Settings templates available for applications listed below		
	▪ Windows Explorer	General ▪ Folder General, Folder View Vista or later only ▪ Folder Search XP and 2003 only ▪ Offline Files
	▪ User Certificates	▪ XP/2003 ▪ Vista or later
	▪ Windows Messaging Subsystem	▪ XP/2003 ▪ Vista or later
Instant Messaging	▪ AOL Instant Messenger	
	▪ Microsoft Lync	▪ 2010, 2013
	▪ MSN Messenger	▪ 7.0, 7.5
	▪ Skype	Up to and including version 6
	▪ Windows Live Messenger	▪ 2011
	▪ Yahoo! Messenger	Up to and including version 11
Internet Browsers	▪ Google Chrome	Up to and including version 30
	▪ Internet Explorer	▪ 6, 7, 8, 9, 10
	▪ Mozilla Firefox	Up to and including version 25
	▪ Opera	▪ Opera 12 or lower ▪ Opera 15 or later
Microsoft Office	▪ Microsoft Access, Excel, Outlook, PowerPoint, Publisher, Word	▪ 2003, 2007, 2010, 2013
	▪ Microsoft FrontPage	▪ 2003
	▪ Microsoft Groove	▪ 2007
	▪ Microsoft InfoPath	▪ 2003, 2007, Designer 2010, Designer 2013, Filler 2010, Filler 2013
	▪ Microsoft OneNote	▪ 2007, 2010, 2013
	▪ Microsoft Project	▪ 2003, 2007, 2010
	▪ Microsoft SharePoint	▪ Designer 2007, Designer 2010, Workspace 2010
	▪ Microsoft Visio	▪ 2003, 2007, 2010
	▪ Office Communicator	▪ 2007
	▪ Microsoft Office Common	▪ 2003, 2007, 2010, 2013
	▪ Microsoft Office Tools	▪ 2003, 2007, 2010, 2013
Other Applications	▪ Adobe Acrobat Professional, Adobe Reader	▪ 6, 7, 8, 9, X, XI
	▪ Adobe Dreamweaver, Illustrator, Photoshop	▪ CS5, CS6
	▪ FileZilla	Up to and including version 3
	▪ Foxit Reader	▪ 5, 6
	▪ iTunes	Up to and including version 11
	▪ Outlook Express	
	▪ Quicktime Player	▪ XP/2003 ▪ Vista and Higher

User Settings templates available for applications listed below		
	▪ WinRAR	Up to and including version 5
	▪ WinZip	Up to and including version 17

Configuration

The User Settings templates for applications contain predefined Targeted Items for a specific application or Microsoft Windows setting and can assist with configuring User Settings.

Notes

- There are some known limitations when using Application Templates:
  - Windows Themes templates are supported on Microsoft Windows Vista and Microsoft Windows 7.
    - Pictures that are saved on a local machine will not be roamed.
    - Custom installed mousepointers will not be roamed, unless they are saved in the folder `%LocalAppData%\Microsoft\Windows\Themes\YOURTHEME\cursors` and the `.theme` file is adjusted to take the cursor from that folder.
    - Aero-specific settings will not be applied to non aero-capable sessions (aero-specific settings will be saved).
  - Device/Hardware related settings are not supported.
  - Settings that require administrative privileges are not supported.
  - The **input language** template is not supported on Microsoft Windows 7.
- It is recommended to use the **Microsoft Office Common** templates on global level.
- **Composition > Applications > Settings > Disable Active Setup (skips first-time shell init)** should be unchecked for Microsoft Windows settings to function properly.
- When at **Composition > Applications > Settings**, **Disable Active Setup (skips first-time shell init)** is selected the following command must be added at **Composition > Actions by Type > Execute Command**: %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall %SystemRoot%\system32\themeui.dll.
- Windows Themes settings will be captured in RES Workspace Manager sessions on Terminal Servers, but due to technical restrictions on a multi-user platform the Desktop Window Manager will not be notified of these settings.

When adding a User Setting, use one of the following methods:

- Click **New > Templates** to use a predefined template.
- Click **New > Discover User Settings...** to start the **User Settings Capture Wizard** that discovers which files and registry settings need to be captured as User Settings for applications or processes.
  Please note that a full installation of RES Workspace Manager is necessary to run the **User Settings Capture Wizard** as the wizard makes use of the RES Workspace Manager drivers. Also, to avoid conflicting results, no RES Workspace Manager session may be running on the system on which the **User Settings Capture Wizard** runs.
- Click **New > Custom** to create your own User Setting.

The following options are available when adding the User Setting (either Custom or by using a Template, or after the User Settings Capture Wizard has finished):

- On the **Capturing** tab, create a list of all the settings to be preserved. If you use a template or the **User Settings Capture Wizard**, this list is already pre-populated.
- When adding or editing Captured items:
- At **Limit # of files to**, enter the number of User Setting files that must be preserved for the managed application. This setting only applies to: Folder/Folder tree.

- Select **Empty target when applying user setting** to delete the corresponding User Setting before applying the setting. This setting only applies to: Registry key/Registry tree/Folder/Folder tree. Normally, targeted items are merged into the existing contents of the registry or folder structure of the user's session. This leaves intact any existing settings that are not overwritten by a User Setting. Sometime this is not the desired behaviour, for example if an application leaves settings behind that it should have cleaned up. In such situations, enable this option.
- Optionally, select **Show exclusions** to add exclusions to the configured settings, so that parts of the settings are not preserved.
    - Select **Any file larger than** to determine the maximum size of the User Settings files and folders to be excluded and enter a number in KB, MB, GB. This setting only applies to: Files/Folders/Folder tree.
    - Select **Any file unchanged for** to determine the maximum age of the User Settings files and folders to be excluded and enter a number in days or months. This setting only applies to: Files/Folders/Folder tree.
- Click **Add > Import > Flex Profile Kit** to import existing Flex Profile INI files directly into the User Setting.
- When specifying paths and names anywhere in User Settings, you can use:
- wildcards *, ?, [charlist] and [!charlist].
- special folders to specify files, folders or folder trees in the user profile directory, as well as the default Microsoft Windows known folders (also called special folders in Microsoft Windows XP and earlier versions of Microsoft Windows) and any other special folder that may exist on the computers in your environment.

Note

If **Windows Shell shortcut creation** is set to **Replace all unmanaged shortcuts**, this may lead to unpredictable results for global User Settings that preserve information in %desktop%, %startmenu% or %appdata%\Microsoft\Internet Explorer\QuickLaunch. This does not affect application-level User Settings for those folders.

Only applicable to global-level User Settings:

- For Global User Settings it is possible to capture items exclusively by enabling the option **Automatically exclude these targeted items from all other User Settings** that is available on the **Capturing** tab. In a session where such an "exclusive" User Setting applies, all other User Settings automatically handle the captured items as (hidden) exclusions for the duration of the user session.
- After a certain time, things like registry settings tend to grow large. To save disk space and to improve performance drastically, the User Settings will be compressed. In a new Datastore the setting is enabled by default. There is however a contingency: all Agents must be running on RES Workspace Manager 9.5.2.0 or higher.

Warnings

- If any of your Agents runs on a version prior to RES Workspace Manager 9.5.2.0, a message appears stating this. You need to update the Agents concerned for the setting to take effect. If an Agent running an older version of the software is added to an existing environment, a more urgent message appears. Such an Agent must be updated immediately, because it cannot load compressed user settings.
- In case of downgrading an Agent, the captured User Settings will not be restored to their previous uncompressed state.

Note

The compression of User Settings only works when Zero Profile mode is set to **Capture targeted items on session end** at global or application level.

Only applicable to application-level User Settings:

- On the **Properties** tab, with the option **Restore application to default configuration**, the end user or Management Console user can revert an application to its original configuration (only available if the **Zero Profile mode** for the application is set to **Capture targeted items on application/session end** (on the **Capturing** tab)).
- When reverting to an application's default configuration, all previously cached User Settings for the application will be deleted, as well as all preserved registry values, files and folders from the user profile that are related to the application. Before enabling the option **Restore application to default configuration**, it is advised to first test if the application will launch correctly with its default configuration.
- When using the option **Restore application to default configuration**, it is recommended to select the option **Empty target when applying user setting** for the captured settings (only applicable to Registry key/Registry tree/Folder/Folder tree). This will delete any existing settings that are not overwritten by the User Setting, which can be useful in case the application leaves behind settings that it should have cleaned up.
- By default, the settings specified in the application's User Settings are preserved at application end: **Capture: After application has ended**. Optionally, you can set **Capture: After session has ended** instead, to preserve the settings later. To change the default configuration, you need to switch to the **Advanced User Settings** view (**Capturing** tab).
- The **Sampling** tab is only available in **Advanced User Settings** view.
- If an application in this Zero Profile mode runs in sampling mode, its **Sampling** tab shows the settings that users did change during the sampled sessions, but that they subsequently lost because those changes did not fall within the scope of the application's **Targeted Items**.
- The Sampling ratio controls the number of sessions from which information is logged. A higher ratio results in information from more sessions, and a lower ratio results in information from fewer sessions. With the ratio of 1:1, information is shown from all sessions.
- On the **Sampling** tab:
  - settings that are part of a User Setting exclusion are not shown.
  - you can right-click a sampled setting and convert it into a User Setting targeted item or into a **User Registry Setting** (on page 125).
  - use CTRL+F to search for a specific sampling entry.
  - you can group the information by dragging column headers to the grouping area. To restore the original view, drag the column headers back to the column bar.

- The value set for the option **Start sampling** determines when RES Workspace Manager should start sampling data.
    - The default **Start sampling: After application has started and is ready to be used** is useful if the application loads and processes user-related settings after it has started up. Postponing the sampling until the application is ready for use filters out irrelevant changes from the **Sampled data** tab. With this option, changes are only sampled if they are made by this specific managed application.
    - Set **Start sampling: Immediately when application starts** if you want to see sampled data about changes made during the application's startup process. With this option, sampling is active as soon as the session has started. Any changes made by an unmanaged version of this application will also be included in the sampling.
- Select **Use the User Settings from the following application** to link an application to the User Settings of another application, rather than giving the application its own User Settings. Please note that linked User Settings are not supported for Citrix Streamed Applications.

Note

When creating a Managed Application for a Citrix Streamed Application, User Settings are automatically enabled for that application in the Zero Profile Mode **Track specified settings on application start/end**. By default, two User Setting Targeted Items are also created for that application, targeting the applicable (streaming application GUID-based) Folder tree and Registry tree for that application. This covers the most commonly used locations where Citrix Streamed Applications store their settings. You may need to add additional Targeted Items and/or exceptions.

Track any changed setting within scope immediately (global)

Use the Zero Profile mode **Track any changed setting within scope immediately** to preserve all changes made in a tracked registry tree in HKEY_CURRENT_USER, and/or in a tracked folder tree in the user profile directory. This mode is available for global User Settings.

Configuration

- The **Sampling** and **Tracking** tabs are only available in **Advanced User Setting** view.
- The **Sampling ratio** controls the number of sessions from which information is logged. A higher ratio results in information from more sessions, and a lower ratio results in information from fewer sessions. With the ratio of 1:1, information is shown from all sessions.
- In one or both of the fields **Registry to track** and **Folders to track**, restrict the User Setting to a single registry tree in HKEY_CURRENT_USER and/or to a single folder tree in the user profile directory.
- Optionally, use the field **Process(es) to track** to restrict the User Setting so that it only tracks changes made by one or more specific processes.
    - You can enter just a process name (such as `regedit.exe`), or you can specify an exact path (such as `c:\windows\system32\regedit.exe`).
    - Separate multiple entries with a semi-colon (;).
    - If you restrict the User Setting to a process that also uses subprocesses for certain changes, include these subprocesses in the **Process(es) to track** field.
- On the **Excluded Items** tab, create a list of all the settings that should not be preserved.
    - When specifying paths and names anywhere in User Settings, you can use:
    - wildcards *, ?, [charlist] and [!charlist].
    - special folders (see **Variables and special folders** (on page 158)) to specify files, folders or folder trees in the user profile directory, as well as the default Microsoft Windows known folders (also called special folders in Microsoft Windows XP and earlier versions of Microsoft Windows) and any other special folder that may exist on the computers in your environment.
    - Select **Any file larger than** to determine the maximum size of the User Settings files and folders to be excluded and enter a number in KB, MB, GB.

Sampling

- If the **Sampling Mode** is enabled (only available in **Advanced User Settings** view), the **Sampling** tab shows the settings that were preserved and/or applied during the sampled sessions.
- On the **Sampling** tab:
- settings that are part of an Excluded Item are not shown.
- right-click a sampled settings and convert it into an Excluded Item or into a User Registry Setting.
- use CTRL+F to search for a specific sampling entry.
- You can group the information by dragging column headers to the grouping area. To restore the original view, drag the column headers back to the column bar.

Note

- If Windows Shell shortcut creation is set to Replace all unmanaged shortcuts, this may lead to unpredictable results for global User Settings that preserve information in %desktop%, `%startmenu%` or `%appdata%\Microsoft\Internet Explorer\QuickLaunch`. This does not affect application-level User Settings for those folders.
- If changes handled by a subprocess should be included in the tracking and sampling of a global User Setting in the Zero Profile mode **Track any changed setting within scope immediately**, the subprocess must be authorized at **Security > Global Authorized Files**.
- When testing User Settings, please note that manually renaming registry keys may lead to unexpected results. To test User Settings, always use the proper application or Microsoft Windows feature to implement changes.

Track any setting changed by application immediately (application)

Use the Zero Profile mode **Track any setting changed by application immediately** to preserve all changes that the application's process makes in the registry at HKEY_CURRENT_USER and to files and folders in the user's `%appdata%` folder.

Configuration Advanced User Settings

- The **Tracking** and **Sampling** tabs are only available in **Advanced User Settings** view.
- If an application in this Zero Profile mode runs in sampling mode, its **Sampled Data** tab shows the settings that were preserved and/or applied during the sampled sessions.
- The **Sampling ratio controls** the number of sessions from which information is logged. A higher ratio results in information from more sessions, and a lower ratio results in information from fewer sessions. With the ratio of 1:1, information is shown from all sessions.
- The value set for the option **Start tracking changes** determines when RES Workspace Manager should start tracking the changes to be processed.
    - The default **Start tracking**: **After application has started and is ready to be used** is useful if the application loads and processes user-related settings after it has started up. Postponing the tracking until the application is ready for use filters out irrelevant changes from the **Sampled Data** tab. With this option, changes are only tracked if they are made by this specific managed application.
    - Set **Start tracking** to **immediately when application starts** if relevant changes are made during the application's startup process. With this option, tracking is active as soon as the session has started. Any changes made by an unmanaged version of this application will also be tracked.
- On the **Tracking** tab:
    - Create a list of all the settings that should not be preserved.
    - When specifying paths and names anywhere in User Settings, you can use:
        - wildcards *, ?, [charlist] and [!charlist].
        - special folders (see **Variables and special folders** (on page 158)) to specify files, folders or folder trees in the user profile directory, as well as the default Microsoft Windows known folders (also called special folders in Microsoft Windows XP and earlier versions of Microsoft Windows) and any other special folder that may exist on the computers in your environment.
    - You can specify any **Extra process(es) to track**. This can be useful in case applications use subprocesses.
    - Select **Any file larger than** to determine the maximum size of the User Settings files and folders to be excluded and enter a number in KB, MB, GB.

- On the **Sampling** tab:
  - settings that are part of an Excluded Item are not shown.
  - right-click a sampled settings and convert it into an Excluded Item or into a User Registry Setting.
  - use CTRL+F to search for a specific sampling entry.
  - You can group the information by dragging column headers to the grouping area. To restore the original view, drag the column headers back to the column bar.

Notes

- A User Setting for a specific application is never available to users who do not get the application itself. If Access Control and Workspace Control are set on an application-based User Setting, users only get the User Setting if they meet both the criteria for the application and the criteria for the User Setting.
- If the subprocess is listed on the **Authorized Files** tab of the application's Security section, the subprocess will be processed and, if relevant, sampled as part of the application-level User Setting.
- If the subprocess is listed at **Security > Global Authorized Files**, changes made through this subprocess will be processed as part of the application-level User Setting, but will not be included in the application's User Setting sampling.
- Application-level Authorized Files are not included in User Setting linking. If an application links to the User Settings of another application, the Authorized Files of the master application must be added to the linked application manually.
- When testing User Settings, please note that manually renaming registry keys may lead to unexpected results. To test User Settings, always use the proper application or Microsoft Windows feature to implement changes.
- With User Settings tracking for applications, in a mixed environment of RES Workspace Manager Console 2012 SR2 or higher and RES Workspace Composer 2012 SR1 or earlier, subfolders of %LOCALAPPDATA%, e.g. %LOCALAPPDATA%\Microsoft, will not be tracked.

7.6.2 Migration settings when switching to another Zero Profile mode

User Settings data is stored in different formats for different Zero Profile modes. When switching an existing global User Setting or application to another Zero Profile mode, use its **Migration settings** to determine what should happen to data stored in the previous format.

Migration Settting "Ignore"	
Effect:	The old data continues to exist, but it is not used or updated. When users start using the switched User Setting, they will initially get the default settings and they will gradually build up a new set of data according to the new Zero Profile Mode. Eventually, two sets of data will exist for each user for both Zero Profile Modes. In that situation, switching the Zero Profile mode results in a switch to the stored settings appropriate to the current mode.
Other consequences:	Additional data remains in the system and, when not using User Settings caching, will be transferred at various moments (session logon, logoff and, refresh; and application start and end). This could potentially impact performance.
Migration Settting "Remove"	
Effect:	All the old information is permanently deleted. At their next logon, users get the default settings and will have to re-do any changes they want in their profile. These changes will then be stored according to the new Zero Profile Mode.
Other consequences:	
Migration Setting "Apply/Convert and remove"	
Effect:	The existing data is converted into the new format. The data is no longer available in the previous format. When users next log on, they will have the customized settings that they already had.
Other consequences:	The new User Setting may store more information than would strictly be necessary. This additional data will be transferred at various moments (session logon, logoff and, refresh; and application start and end).

7.6.3 What is saved as part of a Targeted Item

A Targeted Item for a:	saves:	but does NOT save:
Registry tree	all the keys and subkeys in the specified tree, and the values in those keys	
Registry key	the specified key and all the values in it	subkeys and their values
Registry value	the specified value	▪ other values in the same key ▪ subkeys and their values.
Folder tree	all the files and folders in that tree, including subfolders and their files	
Folder	the specified folder and its file	subfolders and their files
File	the specified file	▪ other files in the same folder ▪ subfolders and the files in them

Notes

- In all cases, parent keys or parent folders will be empty, except for the keys or folders in the path to the User Setting to be stored.
- If you set a registry key as exception to a User Setting, the values in that key will NOT be stored, but any subkeys and their values will.
- If you set a folder as exception to a User Setting, the files in that folder will NOT be stored, but any subfolders and their contents will.

7.6.4 Storage of users' User Setting data

Storage method

Each User Settings is stored as a separate (compressed) file with a GUID as its file name, and with a file extension that indicates its content type.

If the option **Allow users to restore their own settings** is enabled, additional files may be created with sequence numbers related to the value set for **Number of sessions to keep**.

Application-level User Settings with "Track specified settings on application start/end"	
GUID:	GUID of the individual Targeted Item
File name:	▪ [GUID].UPR for registry information ▪ [GUID].UPF for file and folder information
Data for rollback:	Contained in additional files with a sequence number per session: ▪ [GUID].UPR_h[n] ▪ [GUID].UPF_h[n] (where [n] is the session number)
Application-level User Settings with "Track any setting changed by application immediately"	
GUID:	GUID of the application
File name:	▪ [GUID].UPR2 for registry information ▪ [GUID].UPF2 for folder tree information
Data for rollback:	All data, including rollback data, is contained in a single file.
Global User Settings with "Track specified settings on session start/end"	
GUID:	GUID of the individual Targeted Item
File name:	▪ [GUID].UPR for registry information ▪ [GUID].UPF for file and folder information
Data for rollback:	Contained in additional files with a sequence number per session: ▪ [GUID].UPR_h[n] ▪ [GUID].UPF_h[n] (where [n] is the session number)
Global User Settings with "Track any changed setting within scope immediately"	
GUID:	GUID of the User Setting
File name:	▪ [GUID].UPR2 for registry information ▪ [GUID].UPF2 for folder tree information
Data for rollback:	All data, including rollback data, is contained in a single file.

Central storage location of User Settings and other user-specific information

In a user's session, the central storage location stores the file `PWRUSER.ini` and other user-specific information. User Settings files are stored in a subfolder (`\UserPref`) of the central storage location.

The central storage location is defined on the **Settings** tab at **Composition > User Settings**, at **Central storage location**.

The default central storage location is the hidden folder `\Personal Settings` on the user's homedrive. Its location can be customized to:

- A mapped network drive letter and folder name.
- Any path in UNC format.

Environment variables from both Microsoft Windows and RES Workspace Manager can be used. Always ensure that this path is unique per user, for example by including %username%. (Otherwise, files from multiple users could get mixed together in a single location.)

You can define different locations for different Workspace Models.

Locally cached User Settings (on page 154) files are synchronized to the central storage location automatically at the end of each session.

Note

Support for a UNC path as central storage location was introduced in RES WM 2012 SR1 and is not backwards compatible. Should you need to downgrade to a version prior to that, please first ensure that the central storage location refers to a folder on <homedrive> or on a mapped network drive letter.

Migration

When you change the location for **Storage of user settings**, the value set for **Migration Settings** (also at **Composition > User Settings**) determines what will happen to RES Workspace Manager data currently stored in the original location.

Migration Setting	Effect
Ignore	The stored user settings data remains in the old location, but it is not used or updated. At their next logon, users will initially get the default settings. They will gradually build up a new set of data in the new location. Eventually, two sets of data will exist for each user, in both locations. In that situation, switching the storage location back to previous value results in a switch to the settings that are stored there.
Copy	The stored user settings data is copied to a new location and is used and updated from there. At their next logon, users get their customized settings as usual. The data also remains in the old location, but it is not used or updated there.
Remove	The stored user settings data is removed from the old location. At their next logon, users will initially get the default settings. They will gradually build up a new set of data in the new location.

User Settings Caching

User Settings are always stored centrally, in the **central storage location** (on page 152). Optionally, User Settings can also be cached locally.

Locally cached User Settings are available even if the central location is not available, for example on a laptop that is not logged on to a network. Local caching can also improve performance on persistent desktops, as there is no need to copy a User Setting from the central location to the Agent (unless it has changed since the user's last session). However, cached tracked User Settings are not immediately available across multiple simultaneous sessions. Depending on the configuration of the caching feature, cached files are synchronized at the end of the session.

Caching policy

The User Settings caching policy is determined (per Workspace Model) at **Composition > User Settings > User Settings caching**:

- Cache locally at logon and logoff, unless otherwise specified.
- Cache locally at logon, during the session, and at logoff, unless otherwise specified.
- Do not cache locally, unless otherwise specified.

On a managed application or on a global User Settings container, use the Advanced User Setting option **Override local caching** and choose **Always cache** or **Never cache** to overrule the User Settings caching policy.

Terminal Servers are automatically excluded from all User Settings caching. All sessions on Terminal Servers use User Setting files from the central storage location.

User Settings caching requires at least Microsoft .NET Framework 4.0 Client Profile or higher to be installed on the Agent.

Synchronization between central storage location and cache location

The in-built User Settings synchronization process uses a customized synchronization method that is more efficient than other file synchronization methods, as it is optimized for the User Setting mechanism and file structures.

Synchronization between the central drive and the local cache only takes place if the central storage location is available. Without synchronization, User Settings are not uniformly available across sessions on different devices.

The timing of caching is as follows:

- Global User Setting files are synchronized at session start, session end and optionally during the session at defined cache intervals (ranging from 1 minute to 8 hours).
- Application-level User Setting that are preloaded are synchronized in the background at session start, and when the User Settings are stored. Depending on configuration, this can be at application or session end, or during the session at a predefined cache interval.
- Application-level User Setting that are not preloaded are pre-cached in the background at session start and are synchronized when the application starts and when the User Settings are stored. Depending on configuration, this can be at application or session end, or during the session at a predefined cache interval.

Cache location

The cache location is determined at **Composition > User Settings > Cache location**. The default cache location for User Settings is `%localappdata%\RES\WM\UserPref`. This location is inside the user profile, and is therefore not suitable for environments with mandatory user profiles, or when a fresh user profile is created. In such cases, specify a different path. Always ensure that this path is unique per user, for example by including %username%. (Otherwise, files from multiple users could get mixed together in a single location.)

A cache location must be a folder on the local hard drive of the Agent running the session. If the folder does not exist, RES Workspace Manager will try to create it. If it fails to create the folder, or if the specified cache location is invalid, User Settings caching is not possible. If available, the User Settings will then be retrieved from the central storage location instead.

7.6.5 Additional User Setting options

Sampling

Sampling is an advanced User Setting and only available in the **Advanced User Settings** view.

Run a User Setting in sampling mode to obtain information about which settings are changed by users and/or preserved as a User Setting. Sampled information can help you determine:

- which settings users change, but which are lost. You could consider creating User Settings for these settings.
- which changed settings are preserved for users, while they should instead be kept at their default value. You could consider creating User Setting exceptions for these settings, so that users' changes to these settings are not preserved.
- which settings users always set to specific values. You could consider creating registry setting Actions for these settings to ensure that the desired value is already available for users, depending on their context.

Application-level User Settings

Zero Profile mode	Sampled Data
Track any setting changed by application immediately	shows all the registry, file and folder changes that are preserved. Settings that are excluded are not shown. ▪ Right-click an entry and choose **Convert selected entry to User Setting exclusion** if the setting should not be preserved in future.
Track specified settings on application start/end	shows all the the changes that are made in user sessions but that are not preserved. ▪ Right-click an entry and choose **Convert selected entry to User Setting** if the setting should be preserved in future. ▪ Right-click an entry and choose **Convert selected entry to PowerLaunch setting** if the setting should be set as part of PowerLaunch in future.

Global User Settings

Zero Profile mode	Sampled Data
Track any changed setting within scope immediately	shows all the registry changes that are preserved. Settings that are excluded are not shown. ▪ Right-click an entry and choose **Convert selected entry to User Setting exclusion** if the setting should not be preserved in future.
Track specified settings on session start/end	is not available.

Sampling ratio

The **Sampling ratio** controls the number of sessions from which information is logged, and therefore it controls the amount of data shown on the **Sampled Data** tab. Optionally, set a higher ratio to view information from more sessions, or set a lower ratio to see information from fewer sessions. With the ratio of 1 out of 1, information is shown from all sessions.

The Event Log in a user's Workspace Analysis shows whether sampling was active during a specific session.

Notes

- To include an application subprocess in an application-level User Setting in the Zero Profile mode **Track any setting changed by application immediately**, the subprocess must be listed as an Authorized File:
  - If the subprocess is authorized on the **Authorized Files** tab of the application's **Security** section, the subprocess is included in the application's **Sampled Data**.
  - If the subprocess is listed at **Security > Global Authorized Files**, changes made by this subprocess are preserved as part of the application-level User Setting, but are not shown in the application's **Sampled Data**.
- If files, folders or folder trees containing User Settings are excluded based on size and/or date at **Composition > Applications** on the **User Settings > Tracking** tab, these will be added when the application is in sampling mode, but with the note that they will be excluded due to size and/or date.

Linking

If several applications need the same set of User Settings, you do not need to configure this set for each application. Instead, an application can use the User Settings of another application. When the set of User Settings changes, all the applications that use these User Settings will automatically reflect these changes too. This saves configuration and maintenance time, and ensures that multiple applications have identical User Settings.

This is useful, for example, if you need a duplicate of an existing application in order to test out a new version of the application. Another example could be two applications that use the same SQL database.

- The application with the original set of User Settings cannot itself use the User Settings of another application.
- When you edit linked User Settings, RES Workspace Manager will open the application from which the User Settings originate.
- The application with the original set of User Settings cannot be deleted while other applications still use its User Settings. When you unlink an application, you can choose whether to create a copy of these User Settings for the application.
- When you create a Building Block containing an application that is linked to the User Settings of another application, the Building Block will recreate this link when importing the Building Block again. If necessary, it will also recreate the application from which the User Settings originate.
- If the source application uses Zero Profile mode **Track any setting changed by application immediately** with Authorized Files to track changes made by application subprocesses, these Authorized Files must be added to the linked application manually.
- Linked User Settings are not supported for Citrix Streamed Applications.

Allow users to restore their own settings

An application-level or global User Setting becomes available for rollback in the **Restore User Settings** wizard if the option **Allow end users to: Restore settings from previous session(s)** is selected for that User Setting AND if the user has actual stored settings for that User Setting.

For applications, if the option **Restore application to default configuration** is selected, the user can revert the application to its original configuration.

The **Restore User Settings** wizard is available on the **Other** tab of the user's "Workspace Preferences" tool.

The **Restore User Settings** wizard can also be made available as a separate application in the user's workspace. To do so, create a Managed Application that refers to `pwrgate.exe` in its command line with the command line parameter `-15`.

It is also possible to restore a user's User Setting to a previous value from the Workspace Manager Console. This allows the administrator to remotely revert a User Setting for a specific user to a previous state, without the user having to use the Workspace Preferences tool. For applications, the administrator can also revert to an application's default configuration for a specific user from the Console.

The wizard can be found at:

- **Diagnostics > User Sessions > Context menu**
- **Diagnostics > Workspace Analysis > Workspace Analysis Details > Composition > User Settings > Context Menu**
- **Diagnostics > Workspace Analysis > Workspace Analysis Details > Composition > User Settings > View User Setting**

Notes

- The option **Restore application to default configuration** is only available if the **Zero Profile mode** for the application is set to **Capture targeted items on application/session end**.
- When reverting to an application's default configuration, all previously cached User Settings for the application will be deleted, as well as all preserved registry values, files and folders from the user profile that are related to the application. Before enabling the option **Restore application to default configuration**, it is advised to first test if the application will launch correctly with its default configuration.
- When using the option **Restore application to default configuration**, it is recommended to select the option **Empty target when applying user setting** for the captured settings (only applicable to Registry key/Registry tree/Folder/Folder tree). This will delete any existing settings that are not overwritten by the User Setting, which can be useful in case the application leaves behind settings that it should have cleaned up.

Save printing preference

If printers are made available through user workspace management, you can set RES Workspace Manager to preserve users' changes to their default printer settings. To do so, enable this option at **Composition > User Settings > Save printing preference**.

RES Workspace Manager will handle the technical rules to preserve the correct printer settings for each user.

Applications User Settings

It is possible to change the behavior of the timing of loading User Settings for applications. At **Composition > User Settings** two options are available for prefetching User Settings:

- **Prefetch in background, check on application start**: this is the default behavior. The User Settings for applications are loaded in the background during session startup.
- **Apply on application start (requires managed shortcut)**: the User Settings are not loaded during session startup, only the first time an application starts its User Settings will be loaded.
- On the **User Settings** tab of a Managed Application, you can choose either setting as the default for that application (i.e. make an exception to the set default) or choose the setting that has the **(default)** prefix.
- The setting will then be equal to the one set at **Composition > User Settings** (and will be changed accordingly if the default is modified).

Override local caching

It is possible to change the location where User Settings for applications are stored. The Advanced User Setting **Override local caching**, allows you to set exceptions for specific applications:

- **Always cache locally** - can be used if local caching is disabled on a Global level, but you want to cache User Settings for this application locally.
- **Never cache locally** - can be used if local caching is enabled on a Global level, but you do NOT want to cache User Settings for this application locally.

Variables and special folders

When specifying paths and names anywhere in User Settings, you can use:

- the wildcards *, ?, [charlist] and [!charlist].
- the default Microsoft Windows known folders (also called special folders in Microsoft Windows XP and earlier versions of Microsoft Windows) and any other special folder that may exist on the computers in your environment.
- the following special folders to specify files, folders or folder trees in the user profile directory:

Item	File System Directory
%appdata%	Contains application data for all users. This folder is used for application data that is not user specific.
%cache%	Common repository for temporary Internet files.
%cookies%	Common repository for Internet cookies.
%desktop%	Stores file objects on the desktop.
%favorites%	Common repository for the user's favorite items.
%history%	Common repository for Internet history items.
%localappdata%	Data repository for local (non roaming) applications.
%mymusic%	Common repository for music files.
%mypictures%	Common repository for image files.
%myvideo%	Common repository for video files.
%nethood%	Contains the link objects that may exist in the My Network Places folder.
%personal%	Stores a user's common repository of documents.
%printhood%	Contains the link objects that can exist in the Printers folder.
%programsmenu%	Contains the user's program groups (which are themselves file system directories).
%recentfiles%	Contains shortcuts to the user's most recently used documents.
%sendto%	Contains Send To menu items.
%startmenu%	Contains Start menu items.
%startupmenu%	Corresponds to the user's Startup program group.
%templates%	Common repository for document templates.
%userprofile%	Contains the user profile.

7.6.6 Microsoft App-V applications

Version 4.x

When you create a managed Microsoft App-V 4.x application in RES Workspace Manager on the basis of an OSD file, User Settings are automatically enabled for the application. It will run in the Zero Profile mode Track specified settings on application start/end and it will have a hidden Targeted Item for the folder `%APPDATA%\SoftGrid Client\<SGAPPGUID>`. This is where the application will store all its user-specific changes, in a PKG file containing deltas as compared to the original App-V package.

If you use a App-V package that contains a set of applications, then all the user-specific data for these applications is stored in the same PKG file. In the default setup, this results in a duplication of stored user settings data, because the same file is stored for each application that uses it. To prevent this, disable User Settings for all the applications in the set. Instead, create a single global User Setting to cover the set of applications.

There is a method to achieve this:

- create a global User Setting in Zero Profile mode Track specified settings on session start/end with a Targeted Item for the specific subfolder of `%appdata%\SoftGrid Client` where the PKG file of the relevant App-V package is stored; or, if your RES Workspace Manager site includes several App-V packages containing sets of applications, using this option requires a global User Setting for each package.

Ensure that User Settings are disabled for the applications that are covered by the global User Setting.

Version 5.0

The configuration of User Settings for Microsoft App-V 5.0 applications is similar to installed applications. All Zero Profile modes and User Settings options are supported.

Please refer to **User Settings** (on page 140) for more information on how to configure User Settings.

Notes

- The Zero Profile mode and the Targeted Items can be edited forMicrosoft App-V 4.x applications. To view the hidden Targeted Item and its contents, select **Show all User Settings** and **Show Details** at **Composition > User Settings**.
- When creating Microsoft App-V managed applications, the folder to be captured for Microsoft App-V packages, `%appdata%\SoftGrid Client\<SGAPPGUID>` (specified in the **Data** column on the **Capturing** tab after selecting **Show details**), is predefined and cannot be changed.

7.6.7 Citrix streamed applications

When creating a Managed Application for a Citrix Streamed Application, User Settings are automatically enabled for that application in the Zero Profile mode **Track specified settings on application start/end**. By default, two Targeted Items are also created: one targeting the applicable (streaming application GUID-based) Folder tree, and another targeting the relevant Registry tree for that application. This covers the most commonly used locations where Citrix Streamed Applications store their settings. You may need to add additional Targeted Items and/or exceptions.

Note

Linked User Settings are not supported for Citrix Streamed Applications.

Chapter 8: Integration

This chapter focuses on integration of RES Workspace Manager with other RES Software products and products of 3rd party vendors.

8.1 Alerting

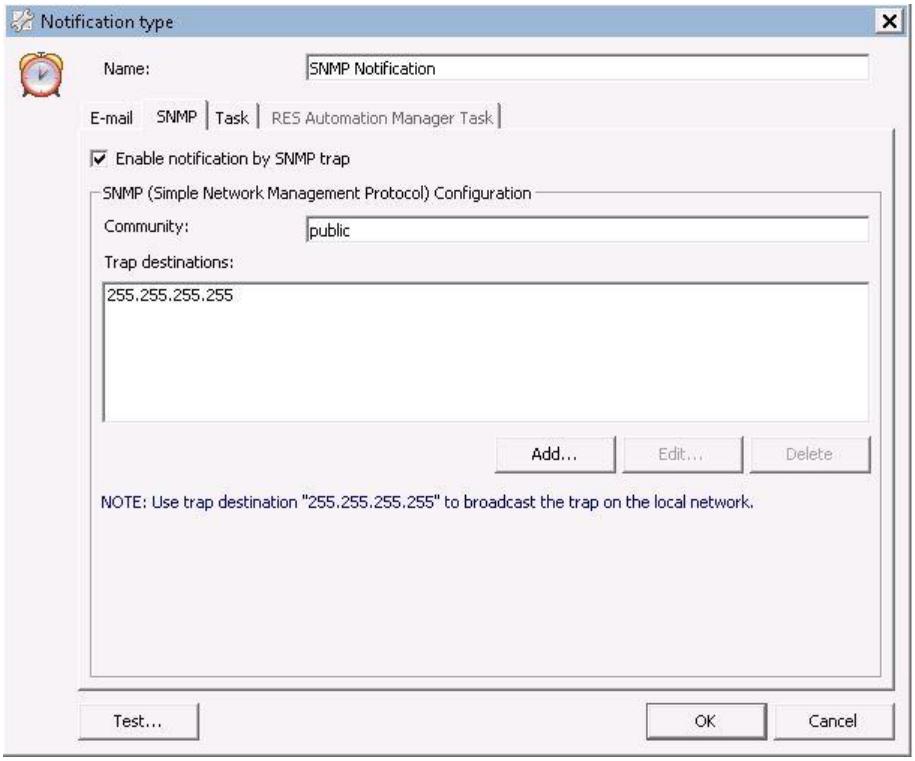
At **Setup > Integration > Alerting**, you can configure automatic notifications about events in your RES Workspace Manager environment. These notifications can consist of **e-mails** to one or more recipients, **SNMP traps** to SNMP system management frameworks, **Commands** and/or **Automation Tasks**. These notification types can then be used to configure the available RES Workspace Manager events.

The events that can trigger Alerting are:

- **Applications**: Errors that occur when a user tries to launch an application.
- **Desktop**: Any events regarding User Installed Applications.
- **Configuration Management**: Any errors occurred in the Event Log.
- **Security Management**: Any event concerning **Application Security**, **Removable Disks Security**, **Files and Folders Security**, **Read-Only Blanketing Security**, **Sessions** and **Network Connections Security**.
- **Performance Management**: Any event concerning **Access Balancing**, **CPU Optimization**, **Memory Optimization** and **Instant LogOff**.
- **Licensing**: Any event concerning the number of available RES Workspace Manager licenses.

Note

The functionality and availability of the Alerting triggers depends on the RES Workspace Manager module.



Note

To receive the SNMP notifications ("traps") correctly in an SNMP framework (such as HP OpenView or CA NSM (Unicenter)), you need to import or load the "respowerfuse.mib" file (in the RES Workspace Manager program folder) into this application. You also need to configure the correct destination for the SNMP traps: use "`255.255.255.255`" to broadcast the trap on the local network or use one or more specific IP addresses to send the traps to one or more specific computers. RES Workspace Manager uses its own mechanism when sending SNMP traps and therefore does not require the installation of SNMP agent software on the computers that run RES Workspace Manager.

8.2 Application Virtualization

Citrix XenApp Publishing (on page 163)

Citrix XenApp Streaming (on page 170)

Microsoft App-V (on page 171)

Microsoft TS RemoteApp (on page 173)

You can also integrate application virtualization solutions other than Microsoft App-V in RES Workspace Manager:

Generic Isolation Integration (on page 176)

8.2.1 Citrix XenApp Publishing

With the RES Workspace Manager **Citrix XenApp Publishing** technology it is possible to create and manage Citrix Published Applications directly from the Console.

Requirements

RES Workspace Manager has two different mechanisms for Citrix XenApp publishing:

- The **local publishing** mechanism is used when the RES Workspace Manager Console is running on a Citrix XenApp server and you publish to the farm to which this Citrix XenApp server also belongs.

  Local publishing is executed by the RES Workspace Manager Console.
- The **remote publishing** mechanism is used when the RES Workspace Manager Console is not running on a Citrix XenApp server, or when the RES Workspace Manager Console is running on a Citrix XenApp server in a different farm than the target farm.

  Remote publishing is executed by the RES Agent Service running on the target Citrix XenApp server.

Publishing a single application or content to multiple farms may trigger both mechanisms.

On each Citrix XenApp server to which RES Workspace Manager will publish, the account running the RES Agent Service must be either local system or a domain account with Full Administration Privileges in the Citrix farm.

For local publishing, the account running the RES Workspace Manager Console must be a user account with Full Administration Privileges in the Citrix farm. For remote publishing, the account running the RES Workspace Manager Console is irrelevant.

If you have Citrix XenApp 6.5 Session Host Only servers (Worker) configured in your environment, consider the following requirements:

- RES Workspace Manager must be installed on one or more Citrix XenApp Controllers (Zone Data Controllers). For redundancy purposes it is preferred to have RES Workspace Manager installed on two or more Citrix XenApp Controllers.
  This is required for the following:
- To retrieve available Citrix XenApp Worker Groups and make them available in the RES Workspace Manager environment.
- Execute Citrix application publishing in case applications are published from an RES Workspace Manager Console that is running on a Citrix XenApp Session Host Only server.
- For Agents running on a Citrix XenApp Controller, the option **Poll for changes** must be set to **Every 5 seconds** (at **Administration > Agents**, on the **Settings** tab).

Notes

- RES Workspace Manager Console users can only change the Citrix folder to which a specific application is to be published if they are running the Console on a Citrix server AND the account running the RES Agent Service has Full Administration Privileges in the Citrix farm.
- A standard 30-second timeout applies to remote publishing tasks. For Citrix XenApp servers to which managed applications will be published remotely, the Agent setting **Poll for changes** should therefore be set at **5 seconds** (at **Administration > Agents**). A longer interval may cause publishing to fail. The Agent setting **Update agent cache on change** does not affect Citrix XenApp publishing.
- Lingering Citrix XenApp applications started by RES Workspace Manager will not show the status 'lingering' on the Citrix server. This is caused by the way RES Workspace Manager starts Citrix published applications. The Session Lingering feature is a Citrix XenApp 6.5 feature.
- For Citrix Session Prelaunch to work, the following prerequisites need to be met:
  - the Citrix server needs to be configured to launch the Workspace Composer automatically (**Administration > Agents**, on the **Agents** tab, select **Automatic** for **Run Workspace Composer**)
  - a Citrix Receiver needs to be started on the client.

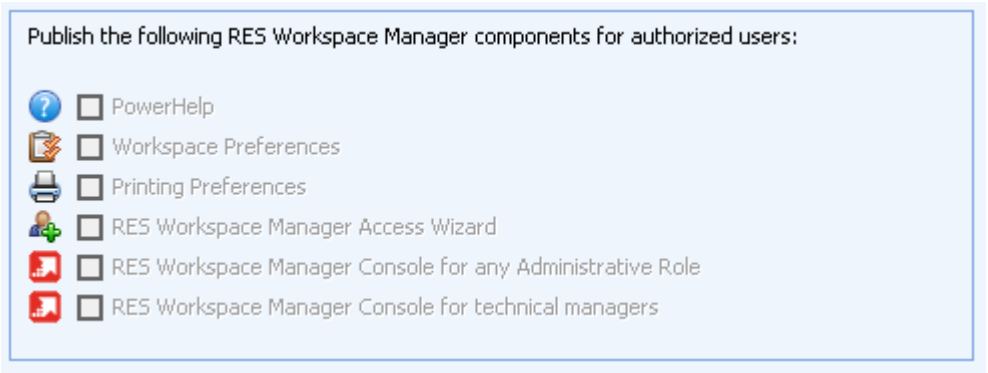
Citrix XenApp Publishing Settings

When setting up Citrix Integration, you first set the correct settings and defaults to use when publishing applications with the Console.

On the **Settings** tab at **Setup > Application Virtualization > Citrix XenApp Publishing**, configure the basic settings of Citrix XenApp Publishing.

- To test whether RES Workspace Manager can connect to a Citrix XenApp server, click **Test Publishing Ability**. If the test is successful, the Console will automatically detect the used Citrix version.
- The **ID used by RES Workspace Manager** is the Citrix XenApp Management Console folder name that is used by RES Workspace Manager when you create published applications. It can be useful to change this ID if multiple RES Workspace Manager Datastores exist in one Citrix XenApp farm. This allows you to keep the published applications unique for each RES Workspace Manager Datastore in the Citrix XenApp farm.
- If OU-based published XenApp applications exist in the user workspace, specify in the field **Rebuild userlist for OU based Published XenApp Applications every day at** when their user list should be rebuilt.

- If a published XenApp application is OU-based, its user list contains all users that belong to the specified OU(s). However, if users are added or removed from these OU(s), these changes need to be reflected in the user list of the published XenApp application. By forcing RES Workspace Manager to refresh this list at the specified time, the Citrix XenApp server can match its user list for the OU-based published XenApp application with the application's current user list, and update it if necessary.
- If an ICA Seamless Host Agent message should be shown when a user logs on, select **Do not suppress message from ICA Seamless Host Agent during logon**. This message is shown if the user connects seamless to a published XenApp desktop via the ICA client and the Terminal Session uses the Microsoft Windows shell. The message is suppressed if the RES Workspace Manager shell is used.
- By default, the option **Use RESPFDIR environment variable in command line of published application** is selected. With this option, Citrix XenApp published applications use the system environment variable %RESPFDIR% in their command line instead of a fixed path to the RES Workspace Manager installation folder. On each Agent, the RES Workspace Manager Agent Service automatically creates %RESPFDIR% and gives it the correct value. This mechanism ensures that the command line works across different Agents with potentially different installation folders.
- On Agents running an older version than RES PowerFuse 2008, please create %RESPFDIR% manually.
- To publish RES Workspace Manager components as a published application in Citrix XenApp, select the relevant options.



- Access to the Access Wizard is automatically restricted to application managers; PowerHelp, Workspace Preferences and Printing Preferences will be available to all users.
- You can create a GPO to configure the RES Workspace Manager desktop as a Citrix XenApp published application.
- Clicking **Add or remove Citrix XenApp servers to or from existing applications** opens a wizard that will guide you through the process, for example, to add a new Citrix XenApp server "CTX10" to all applications that already have Citrix XenApp server "CTX01" in their list of configured Citrix XenApp servers.

Warning

If multiple Citrix Server farms are integrated into your RES Workspace Manager site, the browse window for selecting a folder will show a merged list of all the relevant folders on the relevant farms. If a selected folder does not exist on each farm, the folder will be created there. Please note that Citrix Administrator rights are required to create a new folder on the Citrix server. Otherwise publishing will fail to farms on which the folder needed to be created.

Defaults

The **Defaults** tab can be used to set the default values that will be used when you want to publish **applications** and **content**:

- **Session Window Size**: Configures the size of the session window.
- When selecting a value in the **Colors** field, please note that not all settings listed are supported in all Citrix versions. If a color depth is selected that is not supported by the used Citrix version, the nearest supported color depth will be used.
- **Sound**: Enables or disables sound of the session.
- **Encryption**: Sets the encryption level for the session. If you use Citrix XenApp Secure Gateway, the default encryption level **Basic** should be sufficient.
- Instant Passthrough is a mechanism that provides a shortcut to an application located on a remote server. When a user accesses the shortcut, the request is automatically be redirected to a remote server on which the application is located. See **Instant Passthrough for Citrix XenApp** (on page 168).
- The list of **Available Servers is** populated automatically by RES Workspace Manager. It shows all the site's Server Groups and Agents that are Citrix servers, and all the Citrix Worker Groups from the farms in your RES Workspace Manager site. The list of **Configured Servers** contains all servers, Server Groups and Citrix Worker Groups that you selected to use by default when publishing an application.
- If **Enable Citrix Application Publishing by default** has been selected, the option **Enable "Use Citrix Application Publishing"** will be selected by default when a new application is created.

Server Groups

Click the **Server Groups** tab to configure server groups and assign existing servers to them.

Server Groups are an RES Workspace Manager mechanism to combine multiple Citrix XenApp servers into a single unit. They are typically used to represent silos. After defining a Server Group, you can select this Server Group instead of selecting each individual Citrix XenApp server when publishing an application.

If a group's list of servers changes, any application that references this group will automatically be republished. You can also republish these applications immediately by clicking the **Republish** button.

Publishing Applications

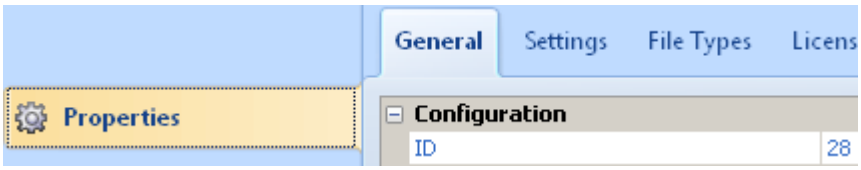
To publish an application with the Console, enable the option **Enable Citrix XenApp Application Publishing** on the tab **Properties > Publishing** of the application window.

On the **Publishing** tab, you can configure specific Citrix properties for the application. When the application is saved, the Console will create the Published Application in the Citrix environment. All options and Access Control types available in RES Workspace Manager are supported for Citrix Published Applications, and will automatically be translated to a correct list of users and groups for the Published Application.

The command line of the Published Application points to RES Workspace Manager with the **application ID** as a parameter so that the application will be managed by RES Workspace Manager. The parent menu structure of the application will be used as the Program Neighborhood Folder property of the application. This property will be modified automatically if the name of a parent menu is modified, or if the application is moved from one menu to the other. If an application is deleted from RES Workspace Manager, and the option **Enable Citrix Application Publishing** was selected, the Published Application will automatically be deleted from the Citrix environment.

Alternatively, you can publish applications as Citrix Published Applications by right-clicking them and selecting **Publish > Citrix XenApp Published Application**. In the Applications list, multiple applications can be selected for publishing using the SHIFT or CTRL keys.

You can manually configure a Published Application to run with RES Workspace Manager. Each application created within the Console has its own unique **ID**. This ID can be found in the **Application Properties** window, on the tab **Properties > General**.



Based on this ID number, you can launch the RES Workspace Manager environment without the RES Workspace Manager desktop: create a Published Application in the Citrix Management Console. Instead of specifying the application executable, enter `pwrstart.exe` with the parameter `/app_pm=[id]`. RES Workspace Manager will only run the specified application and its configured Actions.

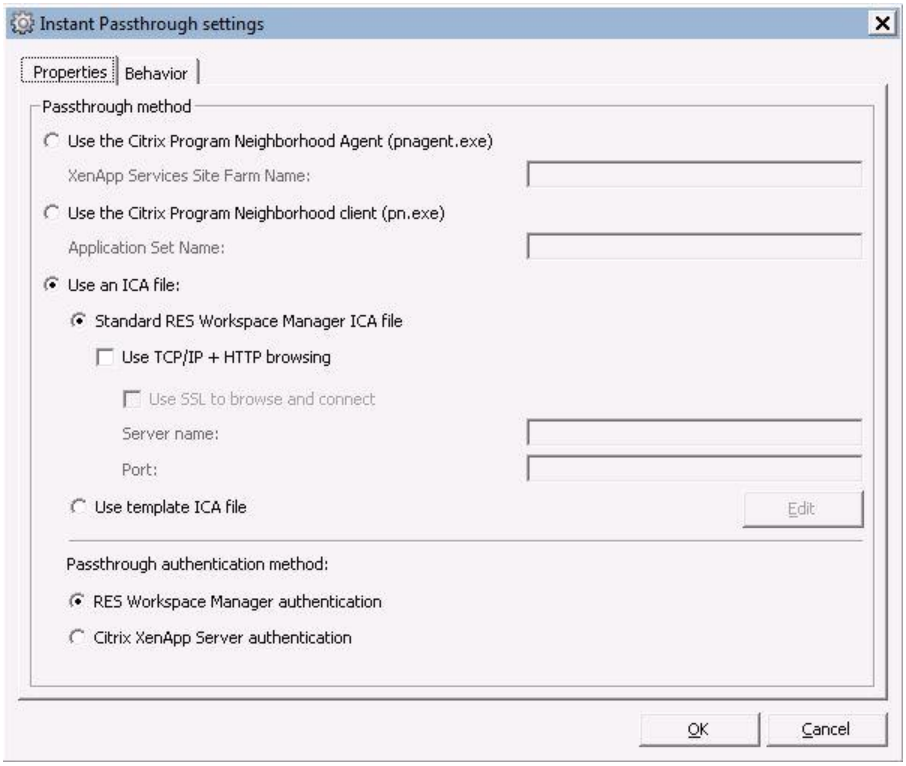
Publishing Content

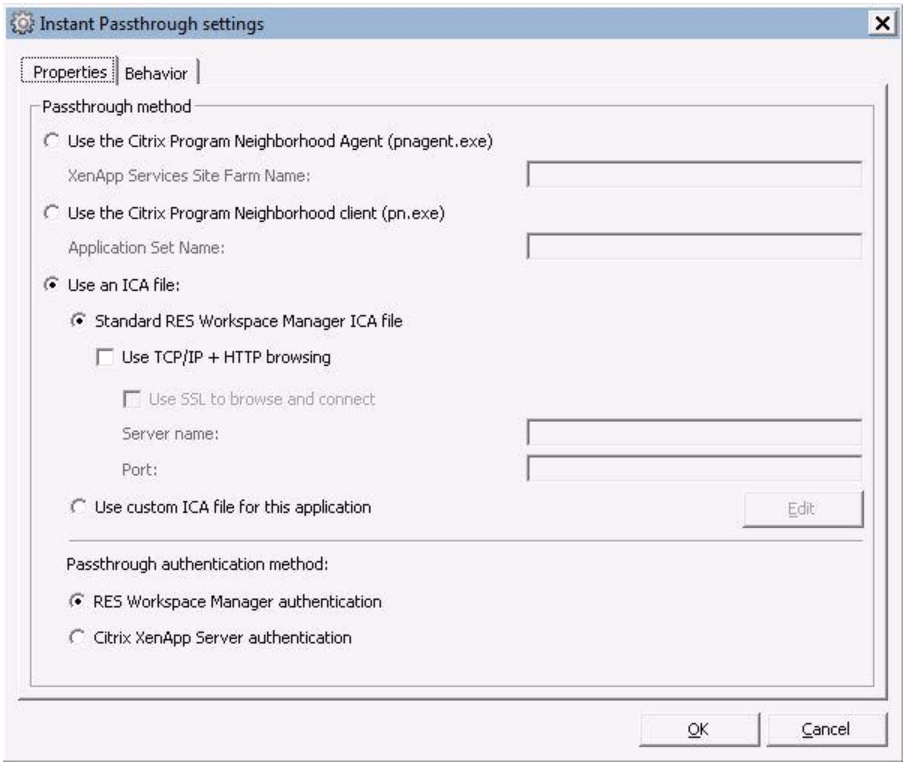
If you select the **Publish as Content** option, the Program Neighborhood configuration options needed for published content will be displayed. Because Content Publishing only requires a command line and access control, all other application configuration options will be disabled.

> **Warning**
>
> If you add Citrix Published Content in RES Workspace Manager, the user should have access rights to this content.

Instant Passthrough for Citrix XenApp

Use the **Instant Passthrough settings** window to configure the Instant Passthrough settings for the entire RES Workspace Manager environment or for a specific application only. This will create an ICA file that will be used to start the Citrix ICA Client. The ICA file is stored in the Datastore.





If the user logs on to a computer on which an application has been published (which is determined by the list of servers on the **Servers** tab of the **Application Publishing** tab of the application), the application will be started directly (i.e. the original command line will be used to start the application).

If the user logs on to a computer on which an application has not been published (again, determined by the list of servers on the **Servers** tab), the application will not be started directly. Instead, the Citrix ICA Client will be started with the ICA file passed as a parameter.

How to configure Instant Passthrough

In the **Instant Passthrough settings** window, you can configure the settings for the passthrough mechanism and the ICA file.

- If you access this window from the global Citrix XenApp Integration node, you are defining the default Instant Passthrough settings for all Citrix XenApp published applications in your environment.
- If you access this window from the Publishing tab of a managed Citrix XenApp published application, the Instant Passthrough settings apply only to that application.

Properties tab

1. To use the TCP/IP+HTTP network protocol to locate and connect to the ICA Server, select **Use TCP/IP+HTTP browsing**.

- To use SSL to locate and connect to the ICA Server, select **Use SSL to browse and connect** and enter the server name and port of the ICA server.

2. Select how passthrough authentication should be handled:

- If RES Workspace Manager handles the authentication, then the parameters `/username`, `/domain`, and `/password` will also be passed to the ICA client with the correct values.
- If Citrix XenApp handles the authentication, then the ICA file will be passed to the ICA Client without any additional parameters.

3. By default, RES Workspace Manager generates an ICA file for each Instant Passthrough connection.

- To create a single custom ICA file for *all* Instant Passthrough connections, select **Use template ICA file** and click [**Edit**]. Please note that this defines a global custom ICA file that will be used for ALL instant passthrough connections, and will overrule any ICA files configured at application level.
- To create a custom ICA file per published application, ensure that the global option **Use template ICA file** is NOT selected. Then, for each Citrix published application for which the default ICA file generated by RES Workspace Manager does not suffice, go to the application's **Publishing** tab, select **Use a custom ICA file for this application** and click [**Edit**].

4. In the **Passthrough method** area, configure how the passthrough should be made available. Launching the passthrough connection using the Citrix Program Neighborhood Client or Agent can be useful, for example, when smartcards are used for authentication:

- **Use the Citrix Program Neighborhood Agent**: if you select this option, the passthrough connection is established by launching `pnagent.exe` with the correct parameters.
- **Use the Citrix Program Neighborhood client**: If you select this option, the passthrough connection is established by launching `pn.exe` with the correct parameters. Because one of these parameters is the name of the application set, you also need to provide this name.
- **Use an ICA file:**
    - **Standard RES Workspace Manager ICA file** or **Use template ICA file**: If you select either of these options, RES Workspace Manager will launch `wfcrun32.exe` using the **Standard RES Workspace Manager** or **template ICA file**.

Behavior tab

With the option **Do not passthrough if application is available on local computer** selected, the published application will only be launched if there is no local version of the application available.

- If the user logs on to a computer on which an application has been published (which is determined by the list of servers on the **Servers** tab of the **Publishing > Citrix XenApp Published Application** tab of the application), the application will be started directly (the original command line will be used to start the application).
- If the user logs on to a computer on which an application has not been published (again, determined by the list of servers on the **Servers** tab), the application will not be started directly. Instead, the Citrix ICA Client will be started with the ICA file passed as a parameter.

You can optionally choose to ignore the configured behavior inside or outside specific Zones via the **Locations and Devices** field.

- If you configure to passthrough anyway **in** specific Zones, at least one of the added Zones must apply.
- If you configure to passthrough anyway **outside** specific Zones, all of the added Zones must apply.

8.2.2 Citrix XenApp Streaming

Citrix Application Streaming Integration allows you to select a `.profile` file directly when adding a Managed Application. If the `.profile` file contains multiple applications, a window is displayed listing all applications and you will be prompted to select one. You still need to prepare the streaming profile of the application. See **Generic Isolation Integration** (on page 176) for more information about preparing streaming profiles.

Notes

- If a Citrix Steamed Application is added User Settings are automatically enabled for that application in the Zero profile mode **Process specified settings on session start/end.** Also two User Settings are created for that application, targeting the applicable (streaming application GUID-based) Folder tree and Registry tree for that application. This covers the most commonly used locations where Citrix Streamed Applications store their settings. Note that exceptions may occur.
- Linked User Settings are not supported for Citrix Streaming Applications.

8.2.3 Microsoft App-V

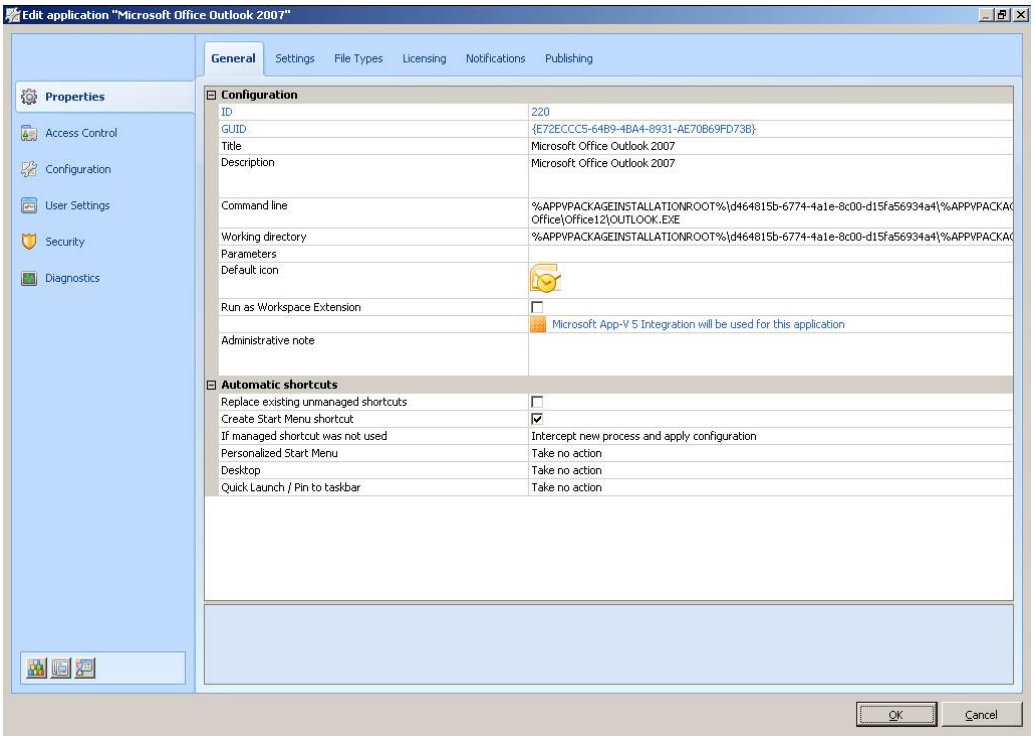
Use the node **Application Virtualization > Microsoft App-V** from the **Setup** menu to configure Microsoft App-V integration. This allows you to integrate virtual applications into your RES Workspace Manager environment.

Version 4.x

To set up a Microsoft App-V application, add an application in the Console and let the command line of the application point to an `.OSD` file.

- The application title, description, Microsoft App-V client version and application icon are automatically retrieved from the `.OSD` file.
- When you save the application, the `.osd` file is copied and modified to provide integration between RES Workspace Manager and Microsoft App-V.
- All RES Workspace Manager technologies will automatically be configured to recognize the application listed in the `.OSD` file.

Please note that the Microsoft App-V 4.x client needs to be installed to be able to retrieve the correct settings from the `.OSD` file.



Version 5.0

To set up a Microsoft App-V 5.0 application, add a new application to the Management Console.

- Specify a title and description for the application.
- The command line can specified in one of these ways:
- If the Microsoft App-V 5 Client is installed on the computer where the App-V 5 application is configured, let the command line of the application point to the executable of a virtual application in the local App-V cache. By default, this cache location is `%ALLUSERSPROFILE%\Microsoft\AppV\Client`. The App-V application GUID and version GUID are included in the command line.
- On Microsoft Windows Vista or higher computers that do not have the Microsoft App-V 5 Client installed, you can point the command line to a manifest file of an App-V 5 application in the shared content folder on the App-V 5 server. This file share has been set up during the installation of your Microsoft App-V 5 server. The command line includes the App-V application GUID and a variable for the version GUID. This ensures that the application will be started even if the App-V package is upgraded.
- Let the command line of the application point to an App-V 5.0 application shortcut (.lnk). RES Workspace Manager resolves the corresponding path and executable, including the App-V application GUID and version GUID.
- The application icon is automatically retrieved from the App-V executable or manifest file.

To configure File Types for the application, click the **Import** button on the **File Types** tab.

With Microsoft App-V 5.0 integration the RES Workspace Manager features that can be configured are extended with User Settings Tracking, User Settings Prefetching, and Process interception.

Notes

- If you create a Building Block of a Microsoft App-V 4.x application and its `.osd` file is stored in the RES Workspace Manager Datastore, the Building Block will contain all information about the contents of the `.osd` file. The `.osd` file will be recreated when the Building Block is used to add or update the application in a different Datastore.
- Changes in the Microsoft App-V Integration will be applied to new sessions only.
- The default virtual Microsoft App-V drive points to "Q:". You can change this for all computers or override this setting for a specific computer or user by setting environment variable `%SGDRIVE%`.
- Microsoft App-V 4.x applications can be set up to run with the `SFTRUN` or the `SFTTRAY` command. However, Microsoft App-V 4.x clients do no longer have the `SFTRUN` command. RES Workspace Manager will now detect this situation and replace the `SFTRUN` on the fly with the command `SFTTRAY /HIDE`. This will help to resolve problems with application definitions when migrating from older Microsoft App-V versions to Microsoft App-V version 4.x.
- If the `.osd` file of a Microsoft App-V 4.x application is stored in the RES Workspace Manager Datastore, you can edit this file if necessary, using any editing tool (e.g. Notepad).
- See http://www.microsoft.com/systemcenter/appv for more information about Microsoft App-V.

8.2.4 Microsoft TS RemoteApp

RES Workspace Manager integrates with the Terminal Services RemoteApp feature of Microsoft Windows Server.

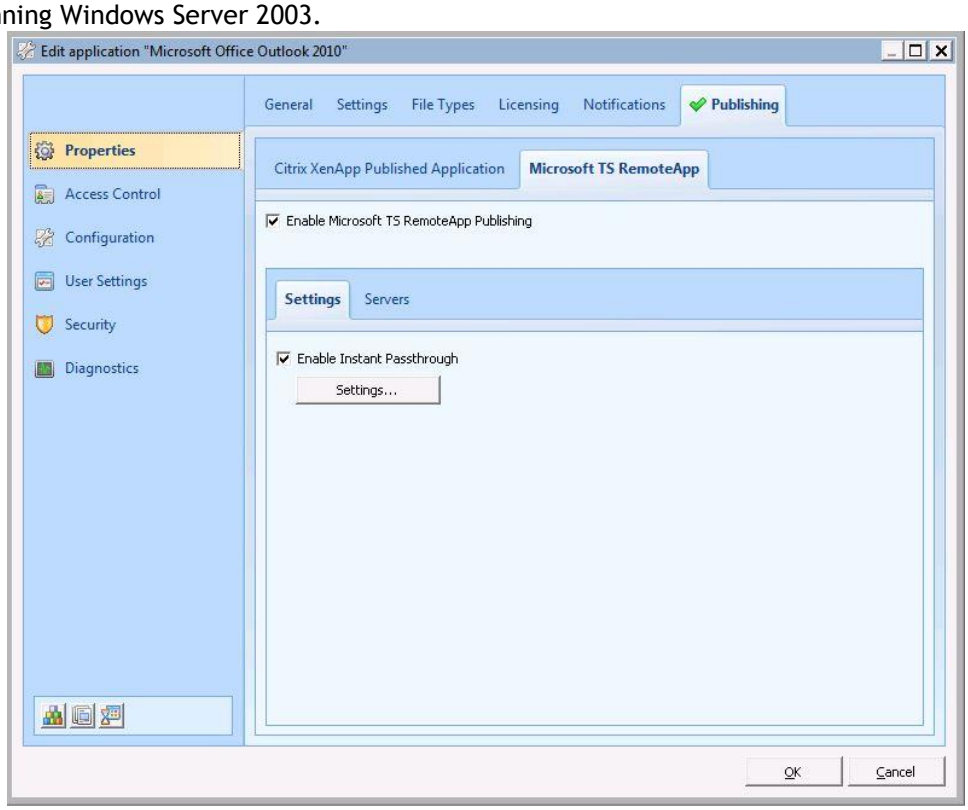
Terminal Services RemoteApp (TS RemoteApp) is a feature that enables users to access applications remotely through Terminal Services. The remote applications appear as if they are running on the user`s local computer. Users can run Microsoft TS RemoteApp applications side-by-side with their local applications. If a user is running more than one Microsoft TS RemoteApp application on the same Terminal Server, the applications will share the same Terminal Services session.

Default values

At **Setup > Integration > Application Virtualization > Microsoft TS RemoteApp** you can configure default values for Microsoft TS RemoteApp deployment, as well as server groups to include specific servers. These server groups can then be used to deploy a Microsoft TS RemoteApp application. The list of available servers will be automatically populated with computers that are running Windows Server 2008 with Terminal Services enabled. You can link a Windows Server 2008 Terminal Server to a Session Broker and be included in a farm to facilitate load balancing between several identical Terminal Servers. When a Windows Server 2008 server is configured to communicate with a Session Broker and is joined to a farm, a server group is automatically created for the farm.

Configuration

To configure an application as a Microsoft TS RemoteApp application, edit the application at **Composition > Applications > Managed Applications** and select the option **Enable Microsoft TS RemoteApp publishing** on the tab **Properties > Publishing**. When Microsoft TS RemoteApp has been enabled, select one or more servers on the **Servers** tab to make the application available as a Microsoft TS RemoteApp application on these servers. The Console does not communicate directly with these servers to create or update the Microsoft TS RemoteApp application. Instead, the RES Workspace Manager Agent process running on the Windows Server 2008 computer will create the Microsoft TS RemoteApp application. Because of this, it is not necessary to configure Microsoft TS RemoteApp from a server running Windows Server 2008: it can also be done from a workstation or a server running Windows Server 2003.



You can also enable **Instant Passthrough** for the application. This will automatically detect whether the application is available directly in a session (if the session is running on a Terminal Server that deploys the application) or whether a terminal session needs to be started to one of the configured Windows 2008 Terminal Servers to start the application as a Microsoft TS RemoteApp application. If a terminal session needs to be started, the RDC client is started with a RES Workspace Manager generated RDP file with the correct information. See **Instant Passthrough for Microsoft TS RemoteApp** (on page 175).

To allow for a seamless user experience, passthrough authentication should be set up in the Windows 2008 Terminal Server environment. Depending on the actual environment, it may be necessary to deploy policy settings or security certificates to enable this. Please refer to Microsoft documentation for the correct procedure.

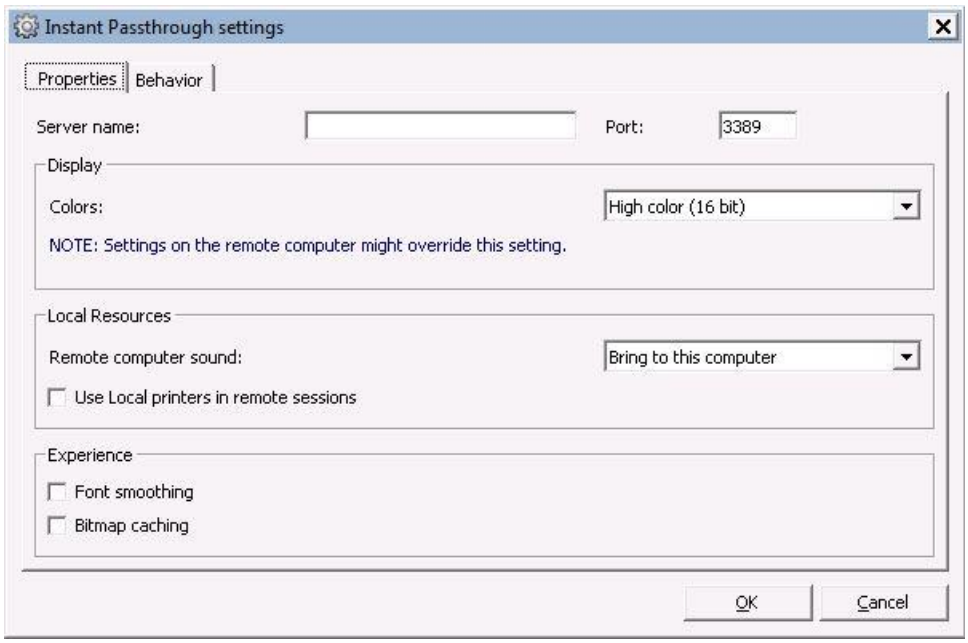
Note

Because of a dependency between the RDC client and the Windows explorer, it is not possible to start a TS RemoteApp application from a session running the RES Workspace Manager shell.

Instant Passthrough for Microsoft TS RemoteApp

Use the **Instant Passthrough settings** window to configure a passthrough mechanism to Microsoft TS RemoteApp applications located on a Terminal Server. This will create an RDP file for each Microsoft TS RemoteApp application. The RDP file points to the application on the Terminal Server and is stored in the DBcache of all specified Terminal Servers in the specified Terminal Server farm. When a user accesses the RDP file, his request will automatically be redirected to the Terminal Server on which the application is located, after which the Terminal Server will deploy the application to the user's desktop.

- If you access this window when configuring Microsoft TS RemoteApp Integration, the Instant Passthrough settings that you configure will serve as the default values for all Microsoft RemoteApp applications in your environment.
- If you access this window when configuring a Microsoft TS RemoteApp application, the Instant Passthrough settings that you configure only apply to the Microsoft TS RemoteApp application.



How to configure Instant Passthrough

- One the **Properties** tab, specify the server name and port of the Terminal Server on which the Microsoft TS RemoteApp applications are located. You can use the name of a Terminal Server, but also the name of a Terminal Server farm. If you want to use single sign-on, you should use the fully qualified domain name.
- In the other fields, specify the behavior of the Microsoft TS RemoteApp application in the RDP session. **Bitmap caching** can speed up your connection by storing frequently used images on your local hard disk.
- On the **Behavior** tab, select **Do not passthrough if application is available on local computer** to define when a published or local version of the application is launched. You can optionally choose to ignore the configured behavior inside or outside specific Zones by using the **Locations and Devices** field.
- If you configure to passthrough anyway **inside** specific Zones, **at least one** of the added Zones must apply.
- If you configure to passthrough anyway **outside** specific Zones, **all** of the added Zones must apply.

Notes

- When an Instant Passthrough session is started from a client running RES Workspace Manager to a Terminal Server, no extra licenses are claimed.
- If a user has logged on to a Terminal Server on which a Microsoft TS RemoteApp application has been deployed and tries to start this application, it will start directly (the original command line of the application will be used to start the application).
- If the user has logged on to a computer or server on which a Microsoft TS RemoteApp application has not been deployed and tries to start this application, an RDP session will be started, based on the values of the Instant Passthrough mechanism.

8.2.5 Generic Isolation Integration

Use Generic Isolation Integration to integrate RES Workspace Manager with application virtualization solutions other than Microsoft App-V (e.g. ThinApp, Citrix).

With Microsoft Application Virtualization integration, you can integrate Microsoft App-V applications into the user workspace. RES Workspace Manager supports Microsoft App-V versions 4.x and 5.0.

Version 4.x

In order to create the integration with App-V 4.x, RES Workspace Manager actively changes the way in which Microsoft App-V applications are invoked. This is done by launching an RES Workspace Manager helper process from within the virtual application environment. This helper process makes configuration changes in the virtual environment (such as registry settings).

Version 5.0

With App-V 5.0 virtual applications work like installed applications, allowing RES Workspace Manager to apply actions and settings to the virtual applications directly. This eliminates the need of a helper process within the virtual application environment and enables User Settings tracking, prefetching User Settings and Process interception in RES Workspace Manager sessions.

You can achieve the same for other solutions, but this requires that you add the integration manually.

Citrix Streamed application integration

Client-side application virtualization reduces the cost of testing, installing and supporting applications. Using isolation and application streaming technologies, client-side application virtualization enables local virtualized applications. Rather than installing applications on user PCs, applications are streamed to a protected isolation environment on their client device.

Steps to take:

- Make the following changes to the streaming profile of the Citrix Streamed application:
  a) Launch the Citrix Streaming Profiler and open the profile of the Citrix Streamed application.
  b) Open **Properties**.
  c) Navigate to **Pre-launch and Post-exit scripts**.
  d) Add Script with following settings:
     - Pre-launch script
     - Isolate script
     - Script location: `c:\program files\res software\workspace manager\pfgii.exe`
  e) Save the changed profile
- Update/Install Citrix Streamed application to target.
- Add Citrix Streamed application to RES Workspace Manager using the Console:

  Using a `.profile` file:

  Command line: `C:\Program Files\Citrix\Streaming Client\raderun.exe`
  Working directory: `C:\Program Files\Citrix\Streaming Client`
  Parameters: `/app:"appliction shortcut name" /package:"unc path\application.profile"`
  E.g.: `/app:"Adobe reader 8" /package:"\\Server\Streamed applications\Acrobat 8XP\acrobat 8XP.profile"`

Note

If you enable **Citrix Application Streaming Integration** at **Application Virtualization > Citrix XenApp Streaming** from the **Setup** menu, you can directly select a `.profile` file when adding a Managed Application manually or by using the Wizard, making this step obsolete. If the `.profile` file contains multiple applications, you will be prompted to select an application.

Using a .rad file:

A .rad file can be created manually with any text editor, such as Notepad.
The file should include the following:

[Rade]
InitialApp=<application which is started by the stream>
PackageLocation=<unc path to the .profile file>

Example:

[Rade]
InitialApp=Adobe reader 8
PackageLocation=\\Server\Streamed applications\acrobat 8\acrobat.profile

Creating the application in the RES Workspace Manager Console:
Command line: C:\Program files\Citrix\Streaming Client\RadeRun.exe
Working directory: C:\Program Files\Citrix\Streaming Client
Parameters: -<Options> "<path>\<streamedapplication.rad>"
E.g.: -C "\\server\Streamed applications\adobe 8XP.rad"

The .rad file can be placed anywhere because it contains a profile location. You can use the Custom Resources Feature in **Administration> Custom Resources** to centrally store these .rad files in the Datastore. The .rad file is than copied to the Agents' local cache when the Workspace Composer is started. When you do this, you also have to change the "path" parameter of this streamed application in the Console so it points to the "%rescustomresources%" location.
E.g.: -C "%rescustomresources%\adobe 8XP.rad"

- Select the option **Use Generic Isolation Integration** at the **Properties** > **Settings** section of a Managed Application for the Citrix Streamed application.

VMWare ThinApp integration:

VMware ThinApp simplifies application delivery by isolating applications from the underlying operating system and plugging directly into existing virtual and physical desktop management tools and infrastructure. ThinApp encapsulates applications inside a Virtual OS that transparently merges a virtual system environment with the real system environment.

Steps to take:

- Make these changes to the capture folder of the Thinstalled application:
  a) Add `respf.vbs` in the root of the capture (where package.ini is located). The `respf.vbs` must contain this text:

```
Function OnFirstParentStart

WaitForProcess
ExecuteVirtualProcess(GetEnvironmentVariable("pwrgrids")),0

End Function
```

  b) Add the following folder to the root of the capture (where `package.ini` is located):

```
%Local AppData%\RES\Workspace Manager
```

- In the RES Workspace Manager folder, add `##Attributes.ini`, containing this text:

```
[Isolation]

DirectoryIsolationMode=Merged
```

- Rebuild the package by using `build.bat`.
- Make the executables located in the \bin folder available, either by placing them on a network share or by distributing them to all computers that run RES Workspace Manager.
- Add the Thinstalled application to RES Workspace Manager using the Console.
- Click the **Settings** tab of the **Properties** section in the **Edit application** window of the Thinstalled application.
- Select **Use Generic Isolation Integration**.

8.3 Microsoft Remote Assistance

RES Workspace Manager fully integrates with Microsoft Remote Assistance. **Microsoft Remote Assistance** allows users (for example helpdesk staff) to quickly remote control a user's desktop and diagnose and repair problems remotely. This decreases resolution time for helpdesks, which in turn decreases their workload.

Remote assistance helpers can remote control workstations and laptops, but not Terminal Servers.

In general, the Operating System on the helper's machine must be equal to or newer than the Operating System on the remote machine. For example, a helper using a Microsoft Windows Vista machine can connect to a Microsoft Windows XP machine, but not to a Microsoft Windows 7 machine.

Prerequisites

- Microsoft Remote Assistance has to be enabled on the computer of the helper and on the remote computer.
- A GPO for "Offer Remote Assistance" has to be created and linked to the computer of the helper and the remote computer.
- On your Microsoft Windows Server, create a GPO:
  - Enable Remote Assistance on this server:
    - Go to **Computer configuration > Administrative Templates > System > Remote Assistance > "Offer Remote Assistance"**.
    - Enable this setting.
  - Configure Remote Assistance:
    - Select "Allow helpers to remotely control the computer" for **Permit remote control of this computer**.
    - Click **Show** to add "Helpers", i.e. Users or Groups that will be allowed access to the computer(s) of other users.
  - Link the GPO:
    - Link the GPO to the computer of the helper and the remote computer.
- Users belonging to a specified helper group must have at least **Read** permissions to the nodes **Microsoft Remote Assistance** in the **Setup** menu and **Diagnostics > User Sessions** in the Management Console.

How to setup Microsoft Remote Assistance

- At **Setup > Integration > Microsoft Remote Assistance**, you can specify which group(s) are allowed to start Remote Assistance sessions and which permissions they have in these sessions.
- Select **Automatically configure Windows Firewall** to adjust the firewall settings to allow Microsoft Remote Assistance.
- At **Diagnostics > User Sessions**, users who belong to a specified helper group can start a Remote Assistance session by right-clicking a user session.

8.4 Microsoft System Center

With **Microsoft System Center ConfigMgr Integration** enabled in RES Workspace Manager, it is possible to deploy software distribution Programs on RES Workspace Manager Agents on which a Microsoft System Center Configuration Manager client is running. It allows you to deliver, install, and configure software at the start of a RES Workspace Manager session or when the user clicks on the application shortcut.

At **Microsoft System Center** in the **Setup** menu, you can integrate the installation feature of Microsoft System Center Configuration Manager in your environment.

Global software distributions can be configured at **Composition > Actions By Type > Microsoft ConfigMgr**. Configure the software distributions for Applications on the **Actions** tab of the **Configuration** section of an application.

Communication

RES Workspace Manager uses Windows Management Instrumentation (WMI) to communicate with both Microsoft Configuration Manager server and client.

When configuring Microsoft System Center Configuration Manager Integration RES Workspace Manager queries the configured Management Server for available software distribution Packages. This is to verify the correct Management Server has been specified.

When configuring Software distributions (Microsoft ConfigMgr), RES Workspace Manager queries the configured Management Server for available software distribution Packages and Programs. After selecting a Program, a reference is stored in the RES Workspace Manager Datastore.

For global software distributions, the RES Workspace Manager Agent creates an advertisement for the selected Program on the Microsoft System Center Management Server at the start of a session. For software distributions configured for an application, the advertisement for the selected Program on the Microsoft System Center Management Server is created when the user starts the application.

The advertisement that was created is based on a temporary Collection that contains only the Configuration Manager client from the computer on which the RES Workspace Manager Agent is running.

The RES Workspace Manager Agent, then notifies the Configuration Manager client about this new advertisement.

If the **Wait for action to finish before continuing** is enabled for a software distribution action for an application, a **Dismiss and notify me when done** notification is displayed in the user session when a user starts the application and the package is deployed. This allows the user to continue working with already available applications while the package is being installed. The user receives a message once the installation is completed.

After deployment of the program, the RES Workspace Manager Agent removes the advertisement from the Management Server.

Warning

Support for Microsoft Configuration Manager 2012 application deployments was introduced in RES Workspace Manager 2014 RC. If you access an RES Workspace Manager 2014 RC (or later) Datastore using an older Management Console, be aware that Microsoft ConfigMgr actions that deploy applications (rather than packages/programs) will be hidden from view.
Important: when accessing an RES Workspace Manager 2014 RC (or later) Datastore using an older Management Console, do not delete any managed application that is configured with a (hidden) Microsoft ConfigMgr 2012 task to deploy an application. Doing so will cause newer Management Consoles to report a Datastore integrity error.

Notes

- Software distributions require a Microsoft System Center Configuration Manager client to be installed on the RES Workspace Manager Agent.
- RES Workspace Manager currently supports distribution of Programs only.
- RES Workspace Manager supports Configuration Manager 2007, 2012, 2012 SP1, and 2012 R2.
- For more information, refer to Microsoft documentation.

8.5 LANDesk

With **LANDesk Integration** enabled in RES Workspace Manager, it is possible to deploy software on RES Workspace Manager Agents on which a LANDesk client is running. It allows you to deliver, install, and configure software at the start of a RES Workspace Manager session or when the user clicks on the application shortcut.

At **LANDesk** in the **Setup** menu, you can integrate the installation feature of LANDesk in your environment.

Global software distributions can be configured at **Composition > Actions By Type > LANDesk**. Configure the software distributions for Applications on the **Actions** tab of the **Configuration** section of an application.

Communication

RES Workspace Manager uses MBSDK Web Service to communicate with LANDesk server.

When configuring LANDesk Integration, RES Workspace Manager queries the configured MBSDK Web Service for available software distribution packages. This is to verify the correct MBSDK Web Service has been specified.

When configuring software distributions (LANDesk), RES Workspace Manager queries the configured MBSDK Web Service for available software distribution packages. After selecting a distribution package, a reference is stored in the RES Workspace Manager Datastore.

For global software distributions, the RES Workspace Manager Agent creates a scheduled task for the selected distribution package on the LANDesk server at the start of a session. For software distributions configured for an application, the scheduled task for the selected distribution package on the LANDesk server is created when the user starts the application.

If the **Wait for action to finish before continuing** is enabled for a software distribution action for an application, a **Dismiss and notify me when done** notification is displayed in the user session when a user starts the application and the distribution package is deployed. This allows the user to continue working with already available applications while the package is being installed. The user receives a message once the installation is completed.

After deployment of the program, the scheduled task will remain on the LANDesk server.

Notes

- Software distributions require a LANDesk client to be installed on the RES Workspace Manager Agent.
- RES Workspace Manager supports LANDesk 9.5 and 9.5 SP1.

8.6 RES Software

At **Setup > Integration > RES Software** you can integrate other RES Software products in RES Workspace Manager.

RES Automation Manager (on page 184)

RES HyperDrive (on page 186)

RES IT Store (on page 187)

RES VDX (on page 188)

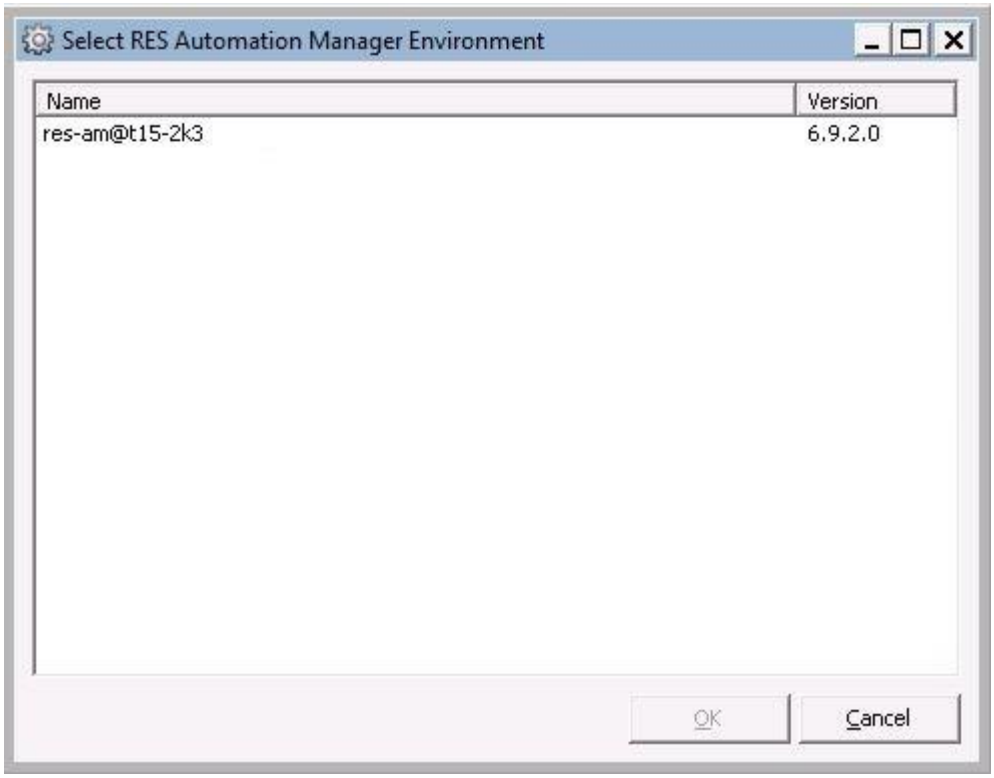
8.6.1 RES Automation Manager

Use the node **Setup > Integration > RES Software > RES Automation Manager** from the **Setup** menu to integrate RES Automation Manager items in your RES Workspace Manager environment. This allows you to run specific Automation tasks in the user workspace, such as the installation of software or the creation of user profiles. RES Workspace Manager will run these Tasks during the logon process of a user. You can configure these Tasks at **Composition > Actions By Type > Automation Tasks**.

You can also use RES Automation Manager Integration to run Automation Tasks as part of an **Alerting** (on page 161) task. You can configure these tasks at **Alerting** in the **Setup** menu.

How to integrate RES Automation Manager in your RES Workspace Manager environment

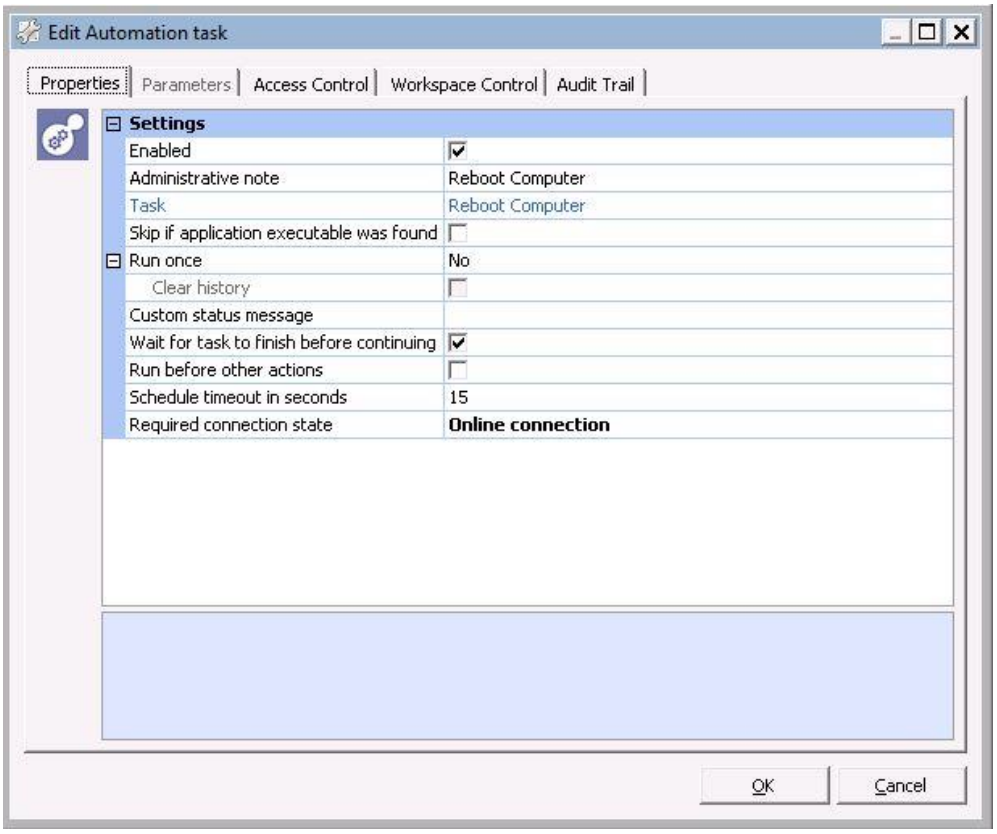
- Click the **Properties** tab to configure integration with RES Automation Manager.
- Select **Enable RES Automation Manager Integration** at the node **Integration > RES Software > RES Automation Manager** from the **Setup** menu
- Click ... to select a RES Automation Manager environment. This opens the **Select RES Automation Manager Environment** window, which allows you to select the RES Automation Manager environment that should be integrated with your RES Workspace Manager environment.



- Select the applicable RES Automation Manager environment and click **OK**.
- Select the authentication method to gain access to the Datastore of the selected RES Automation Manager environment. This should be the same authentication method that is used in RES Automation Manager to gain access to the selected Datastore.
- Select the Dispatcher detection settings that RES Workspace Manager should use to detect the RES Automation Manager Dispatchers.
- When selecting the authentication method to gain access to the RES Automation Manager Datastore, you should use the same authentication method that is used in the RES Automation Manager Datastore.

- When configuring **RES Automation Manager Integration**, you can use the **Test now** button to test if you can actually connect to the selected RES Automation Manager environment.
- The **Log** tab shows a log of all RES Automation Manager actions, including alerting actions.

After configuring RES Automation Manager Integration, you can use RES Automation Manager tasks.



Notes

- When configuring RES Automation Manager Integration, you can only connect to RES Automation Manager environments that run RES Automation Manager Series 4 SR2 or later.
- See http://www.ressoftware.com/products/automation-manager for more information about RES Automation Manager.

Tip

With the **RES Unified Console**, you can easily access the RES Workspace Manager and RES Automation Manager Consoles from a single view.

8.6.2 RES HyperDrive

On the **Settings** tab of **Setup > Integration > RES Software > RES HyperDrive** you can integrate RES HyperDrive into the user workspace. After enabling RES HyperDrive integration client settings can be configured for users running RES HyperDrive. By integrating RES HyperDrive in RES Workspace Manager you can overrule the settings for the RES HyperDrive Client within an RES Workspace Manager session. If no settings are configured the RES HyperDrive Client will run with the user's settings.

Settings

- **RES HyperDrive Client settings** includes all settings that are available in the RES HyperDrive Client. To overrule a setting, select the appropriate value from the list or select <configured> and fill in a value.
- You can override the global settings of this feature for specific Workspace Containers.

The configured settings will be written to the registry at the start of each RES Workspace Manager session and applied from the registry when the RES HyperDrive Client starts.

Note

You are allowed to use environment variables, e.g. `%temp%`, to set numeric or string values.

With **Migrate data from Dropbox to RES HyperDrive** you can configure a one-time data migration from Dropbox to RES HyperDrive. This will invoke the RES HyperDrive Migration Wizard for end users running both RES HyperDrive and Dropbox. The wizard enables these users to mark the business-related (sub)folders stored in their Dropbox and migrate these to the RES HyperDrive of their choice. Optionally, the data can be deleted from Dropbox upon completion of the migration. The Wizard runs at the start of each RES Workspace Manager session until the data migration has been completed, or until the configured migration deadline has been reached. The Wizard only starts if both Dropbox and RES HyperDrive are fully functional.

Notes

- Blocking Dropbox will restrict access to the Dropbox Windows client and the users' Dropbox folder. To block the Dropbox web interface, deny access to the Dropbox website on the **Websites** tab of **Security > Applications > Websites**.
- If the RES HyperDrive Migration Wizard is completed, canceled or cannot be executed, for instance due to no valid RES HyperDrive, an entry is recorded in the RES Workspace Manager Event Log.

8.6.3 RES IT Store

At **Setup > Integration > RES Software > RES IT Store**, you can integrate RES IT Store (formerly known as Service Orchestration) items in your environment.

RES IT Store Integration

RES IT Store Integration allows you to base access to an application or object on the availability of **RES IT Store Services** (already available or created from RES Workspace Manager with the **RES IT Store Service Wizard**). For example, you can base Access Control to the managed application Microsoft Visio on the RES IT Store Service "Microsoft Visio". This enables you to use the RES IT Store workflow to approve and install the application, while RES Workspace Manager automatically makes the managed application available as soon as the service is actually delivered in the end user's workspace.

The **RES IT Store Wizard** is used to create new IT Store services directly from the RES Workspace Manager Console. All communication of this wizard to the Catalog Services of RES IT Store is SSL-encrypted, using port 8081.

Configuration

- Enter the **Catalog host name** and **Port**. The Catalog host is the machine on which the Catalog Services run. The Catalog Services are used by RES Workspace Manager to query which RES IT Store services have been delivered to a user. The default port of the Catalog host is 8080.

  Each user's list of delivered RES IT Store Services is cached to ensure availability of this information in case the Catalog Service cannot be reached.
- Enter the **Publication name** and **password** of the RES IT Store Catalog host. An RES IT Store Catalog host contains a selection of available RES IT Store Services that can be used as Access Principle in Access Control.
- When configuring **RES IT Store Integration**, you can use the **Test now** button to test whether you can actually connect to the specified Catalog host. If connection is possible, an overview of all available RES IT Store Services will be shown.
- Selecting the option **Enable password Reset on Windows logon screen** enables end users to invoke RES IT Store's **Password Reset** feature from the Windows logon screen. This enables end users to reset their Windows password using a Service configured in RES IT Store.

Note

If **Access Control** is based on a **Not RES IT Store Service** rule and **RES IT Store Integration** is disabled, all users will comply with this rule.

Tip

With the **RES Unified Console**, you can easily access the RES Workspace Manager and RES IT Store Consoles from a single view.

8.6.4 RES VDX

At **Setup > Integration > RES Software > RES VDX**, you can enable integration for RES Virtual Desktop Extender. The RES Virtual Desktop Extender merges local applications and a remote desktop into a single workspace. This technology eliminates the need to switch between a local and remote desktop providing an optimized user experience. This is useful if you run applications that do not function properly in a server-based computing environment, or if you have other reasons to keep some applications running locally.

With the RES Virtual Desktop Extender, a virtual channel is created between the session and the locally installed desktop extender as soon as a session is initialized. If the user has been granted access to an application that is installed locally, that application will be presented in the end user's session.

Configuring VDX Integration

To configure an application to run from the local desktop using RES VDX, select **Run as Workspace Extension** at its **Properties > General** tab. (See **Configuring Workspace Extensions**).

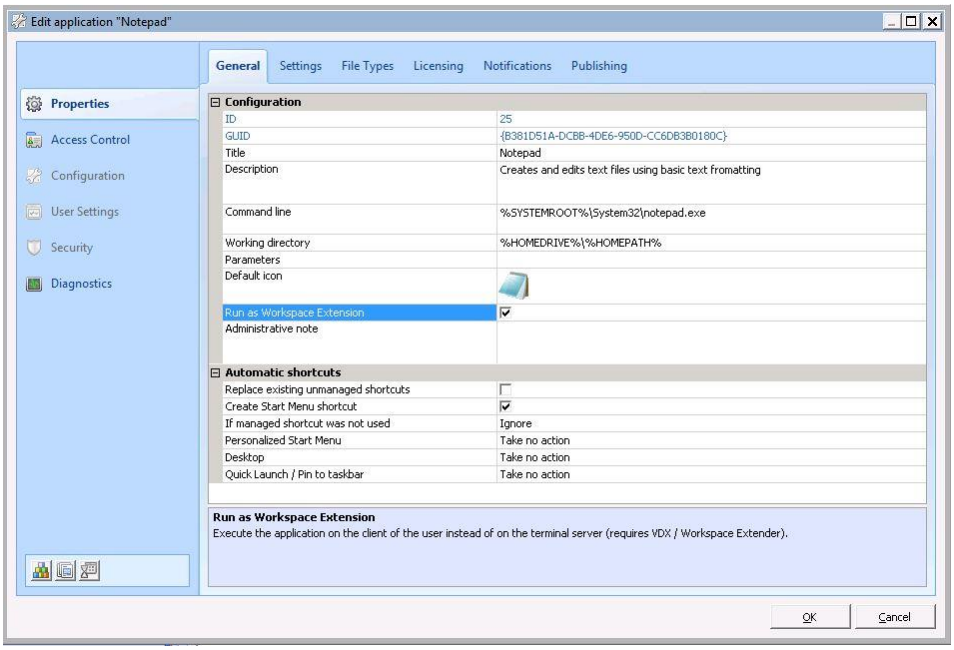
- **Enable RES Virtual Desktop Extender (VDX) integration** - Enable or Disable the integration of RES VDX with RES Workspace Manager. If disabled the VDX functionality remains intact, but is no longer managed by RES Workspace Manager.
- **Enable VDX Engine** - Enable or Disable the RES VDX Engine. This disables VDX altogether, not just the integration with RES Workspace Manager.

Configuring Workspace Extensions

Workspace Extensions are applications that are managed centrally with the Console. If you configure an application to run as a Workspace Extension, it will be displayed in the RES Workspace Manager menu like any other application. The only difference is that you need to specify the local path on the client for the application.

To run an executable on a local workstation as a Workspace Extension in a Centralized Computing session (for example a CAD program), complete the following steps:

- Install the RES VDX client on the client (see RES VDX Documentation for installation and configuration information).
- Create an application with the Console. Select the option **Run as Workspace Extension**.



- Test the configuration by starting the Application.
- Check Usage Tracking to see whether the application usage is logged.

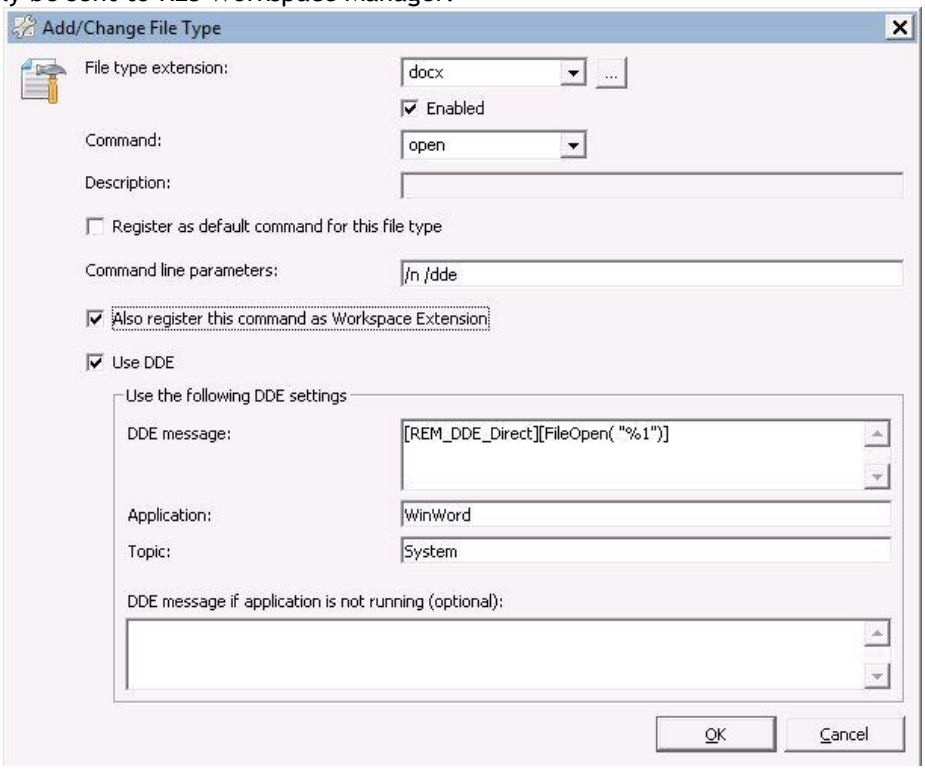
You may also associate the application with a **Zone**:

- Open the Application's properties in the Console.
- Add a Zone at the **Access Control > Locations and Devices** tab.
- Select a previously created Zone or create one.

This restricts the Workspace Extension to a specific Zone. This can be useful, for example, if the application is not locally installed on all workstations. As an alternative, assign the application to a specific **Workspace Container**.

Workspace Extensions and File Types

File Types management integrates seamlessly with Workspace Extensions. If you have configured a file type for an application and selected the option **Register this command as Workspace Extension**, RES VDX will register the file type on the client. If a user double-clicks a file or uses a resource locally for which an association has been made with a central application, the request will automatically be sent to RES Workspace Manager.



8.7 Web Portal

Besides creating a physical desktop by replacing the shell, it is also possible to create a virtual web-based desktop. This allows you to integrate the interface with an existing portal environment for remote access purposes, so that users can connect to their desktop from a remote location via a web interface; and to standardize RES Workspace Manager with other web-based applications in your enterprise.

To create such a web-based desktop, you need to enable Web Portal rendering at the node **Web Portal** on the **Setup** menu. When Web Portal rendering is enabled, RES Workspace Manager will render a Web Portal in the `\Webtop` folder located in the user's temp directory. The Web Portal can be started by launching a web browser with startup parameter `%temp%\webtop\webtop.html`.

You can change the Web Portal's appearance by selecting a Web Portal style. There are three default Web Portal styles to choose from. If you have a basic knowledge of HTML you can edit the Web Portal style to fit your needs.

It is also possible to integrate the Web Portal into an existing portal: To integrate the Web Portal into an existing portal, add a link or frame pointing to the local Web Portal.

You can combine the flexibility of your Web portal with the ease of use of the RES Workspace Manager shell Taskbar: enable Web Portal rendering and then go to **Content > Desktop > Lockdown and Behavior** and select **Hide "Start" button on RES Workspace Manager Shell taskbar**.

Notes

- The Web Portal technology can only be used if Internet Explorer 6 or later is installed.
- Web Portal integration is not enabled by default after the installation of RES Workspace Manager and there is no application Web Portal Integration created automatically as it was in previous versions of RES Workspace Manager. Instead, the Program Files folder of RES Workspace Manager contains a Building Block file `web-portal-integration.xml`. By importing this Building Block file in the Console, you can add the application Web Portal Integration at **Composition > Applications**, so you can offer the Workspace Composer through Microsoft Internet Explorer.

Chapter 9: Tracking and Reporting

In this chapter we will deal with the subject of Tracking and Reporting.

9.1 Usage Tracking

Usage Tracking allows you to monitor application and internet usage in detail, using various selection criteria. Usage Tracking can be used to monitor the actual use of applications per user, per application, or per server.

To configure Usage Tracking, navigate to **Setup > Usage Tracking**

Usage Tracking also lets you monitor active sessions and the actual CPU load of an application. You can use this information to find users or applications that use a more than average amount of system resources, to re-distribute licenses, or simply for troubleshooting.

The following options are available on the **Setup > Usage Tracking** node:

- **Log current activity**: logs all activity in real-time, making it possible to see instantly which users are using which applications.
- **Log history**: if selected, all application usage is logged.
- **Detailed history** logs the following items. This information is shown on the **Details** tab of the Usage Tracking Viewer, and includes specific dates and times:
  - when the application was used
  - by whom
  - for how long
  - on which system
  - what the processor usage was for that application during the time it was used
- **Cumulative history** does not include specific dates and times, but cumulates the application usage data for the specified time. It logs:
  - when the application was used
  - by whom
  - for how long
  - on which system
  - what the processor usage was for that application during the time it was used
    For example, the **Detailed history** logs that someone started Microsoft Word on Monday between 11:00 and 13:00, and on Tuesday between 15:00 and 16:00. The **Cumulative history** only logs that in Week 2012-35 that user had started Microsoft Word for a total of 3 hours (specific dates and times are not shown).

- Selecting the option **Log Session Information** saves all information concerning sessions. The storage duration of the session information depends on the number of days you enter in the **Keep session history** field.
- The option **Anonymous logging** filters user names out of the information provided. This can be used to protect the users' privacy.
- If you want to provide end users and Application Managers with access to Usage Tracking, you can select the option **Enable Usage Tracking access for end-users and application Managers**. A user can only see personal information concerning his own sessions and applications. An Application Manager can only see information related to the applications he manages.
- With the **Enable Website Usage Tracking and log web sites visited by Internet Explorer** option you can keep track of all websites visited by the end user. In Microsoft Internet Explorer (x86/x64) you also need to enable **third-party browser extensions** via **Tools > Internet Options > Advanced > Browsing > Enable third-party browser extensions** or via Microsoft Windows system policies that are set up for your company. Please note that Internet Explorer Enhanced Security Configuration will disable this option by default.
- If you want to make a distinction between different applications with the same name, select **Log path and executable in addition to application name**. This option may be useful when comparing application usage for reporting purposes.

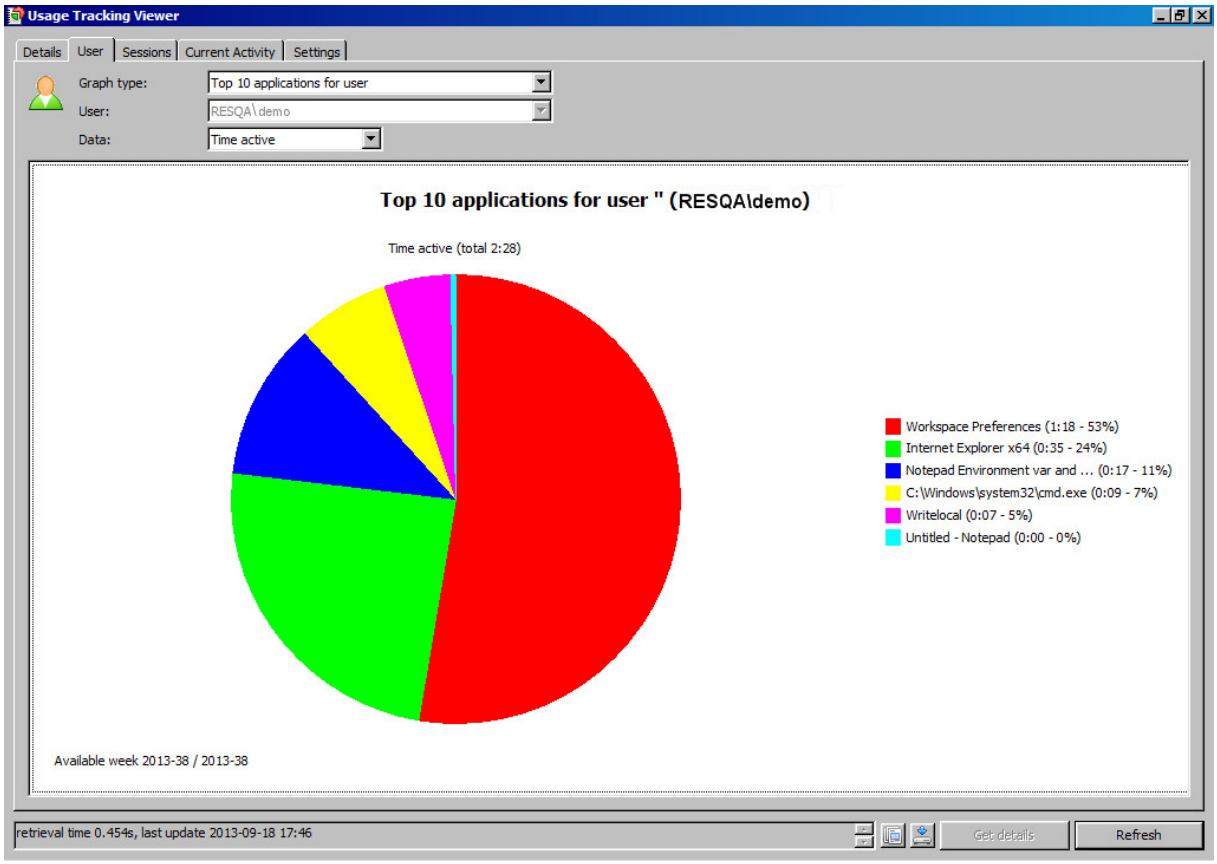
Notes

- In some countries or companies, Usage Tracking can be in conflict with privacy policies. If so, it is advisable not to use Usage Tracking.
- The Usage Tracking database only stores OU information on the lowest OU level. This means that if the OU structure changes, the information displayed by Usage Tracking will change accordingly.
- The Usage Tracking settings **Log current activity**, **Log history** and **Anonymous logging** also apply to Website Usage Tracking.
- If you enable Usage Tracking access for end users, they can view their website usage in the Usage Tracking viewer.
- Internet Explorer running as a Workspace Extension will not be tracked by Website Usage Tracking.

9.2 Usage Tracking Overview

Information gathered by Usage Tracking is presented in the **Usage Tracking Viewer**. The Usage Tracking Viewer can be started from the user's "Workspace Preferences" tool, or from the **Diagnostics > Usage Tracking Overview** node.

You can view a list of detailed information, or you can view a graphical representation of it. For reporting purposes, click  to create an Instant Report (first click **Refresh** to update your data) or  to export data to a file (`.csv` for lists and `.jpg` for graphs).



Notes

- The Usage Tracking Viewer will not display any information about OUs if OU support has not been configured in the Console.
- The Usage Tracking Overview only shows information from the Datastore that is defined at **Setup > Datastore**.
- Computer names of extended applications are preceeded with an asteriks ("*") in the Usage Tracking Overview.

9.3 User Sessions

Use the node **Diagnostics > User Sessions** to display important information about each user that is logged on to your RES Workspace Manager environment.

You can view the following information:

- When was the session started?
- When was the session refreshed?
- What is the idle time of the user?
- What is the state of the user?
- On what client is the user working?
- Which IP address is assigned to the user?
- On what computer is the user working?
- What is the IP address of that computer?
- What Workspace Container is the user working in?
- What is the user's session ID?
- What is the protocol used by the user - ICA, RDP, PCoIP, Blast or Local?
- Is the license in use?
- What is the user's AppGuard mode?
- What is the user's NetGuard mode?
- What is the user's Workspace Composer version?
- What is the user's Workspace Extender version?

If you right-click a user session, the following options are available from the context menu:

Item	Function
Properties	Displays the user properties.
Refresh	Refreshes the Active Users list.
Force refresh of "<user>" now	Refreshes the user's session immediately. This is useful when a refresh is immediately required (e.g. access to a new application was granted or an AppGuard rule was added).
Analyze Workspace of this user	Displays the Workspace Analysis details for the selected user. See **Workspace Analysis** (on page 241).
Ping the user's workstation	Pings the user's computer to determine the network delay to its computer.
Remote Control "<user>"	Allows you to remote control the user's session.
Offer remote Assistance to "<user>"	Allows you start a Remote Assistance session with the user.
Send message to "<user>"	Allows you to send a message to the user.
Log off "<user>"	Allows you to log off the user.
Reset "<user>"	Resets the user's session.
Disconnect "<user>"	Disconnects the user's session.
Restore User Settings	Allows you to restore a user's User Setting to a previous value (from an earlier session) or revert to an application's default configuration.
Create Instant Report	Creates an Instant Report. Depending on your selection, you can also select which items should be included in the Instant report. See **Instant Reports** (on page 234).
Building Block options	Creates Building Blocks. Depending on your selection, you can also select items that should be included in the Building Block(s). See **Building Blocks** (on page 231).
Help	Opens the RES Workspace Manager Help for the **Active Users** node.

Notes

- It is possible to select multiple users to refresh, send a message, log off, reset, or disconnect user sessions. Use the CTRL key to select multiple users, use the SHIFT key to select a range of users, or use CTRL+A to select all users in the list.
- If you group the active users list by server, right-clicking a server will display the option Send message to all users on server <server name>. This allows you to send a user-defined message to all users logged on to the selected server. This option is only available in a Terminal Server environment.
- Some options will only be available for sessions that are logged on to a Terminal Server.

9.4 Workspace Simulation Wizard

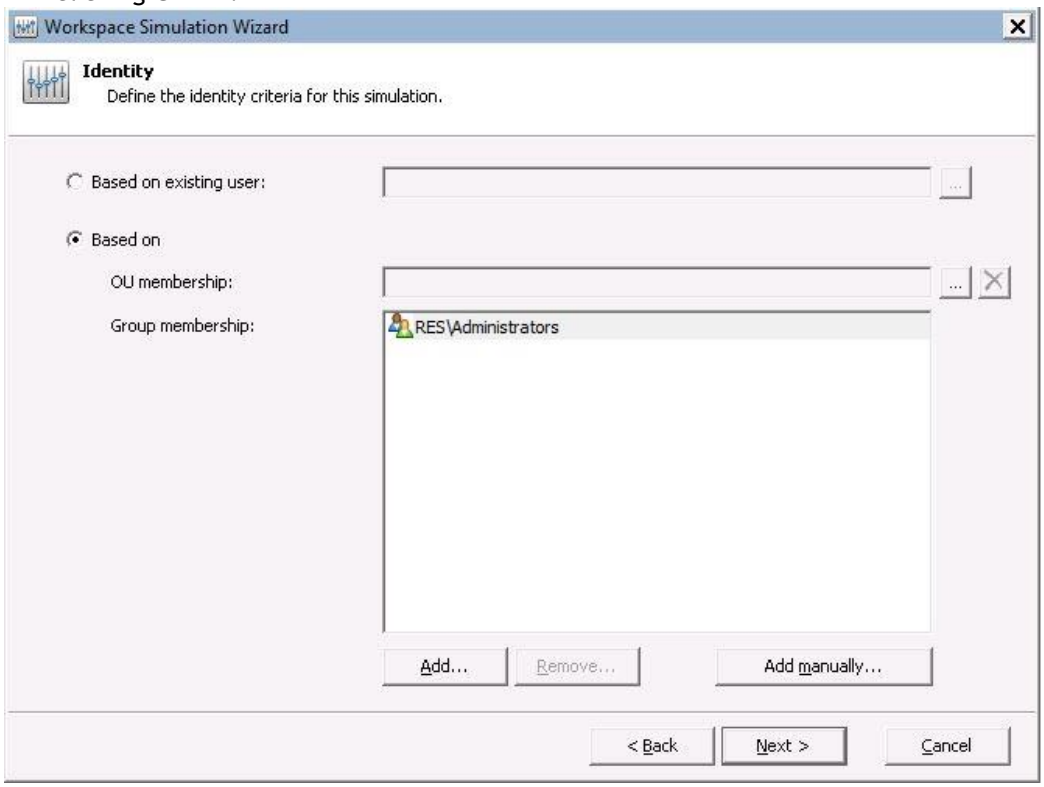
The **Workspace Simulation Wizard** gives you a powerful tool to achieve Desired User State management. Based on identity, locations and Workspace Containers, you can view the Workspace Analysis of a simulated Workspace. For example, by selecting an OU and a number of groups, locations and workspace containers, you can analyze the contents of a Workspace resulting from the specified context. This allows you to predict the composition of a workspace in a particular simulation and to view their impact before actually applying these to your "live" environment.

- The **Workspace Simulation Wizard** can be accessed from any node in the **Diagnostics** section by clicking the **Workspace Simulation** button in the Command bar, or by right-clicking anywhere in the tree view and selecting **Workspace Simulation**. This will start the wizard without a prefilled user identity.
- To start the **Workspace Simulation Wizard** with a prefilled user identity, go to the node **Diagnostics > Workspace Analysis**, select a user and then either right-click and select **Run Workspace Simulation** or click **Action** in the menu bar and select **Workspace Analysis > Run Workspace Simulation**.

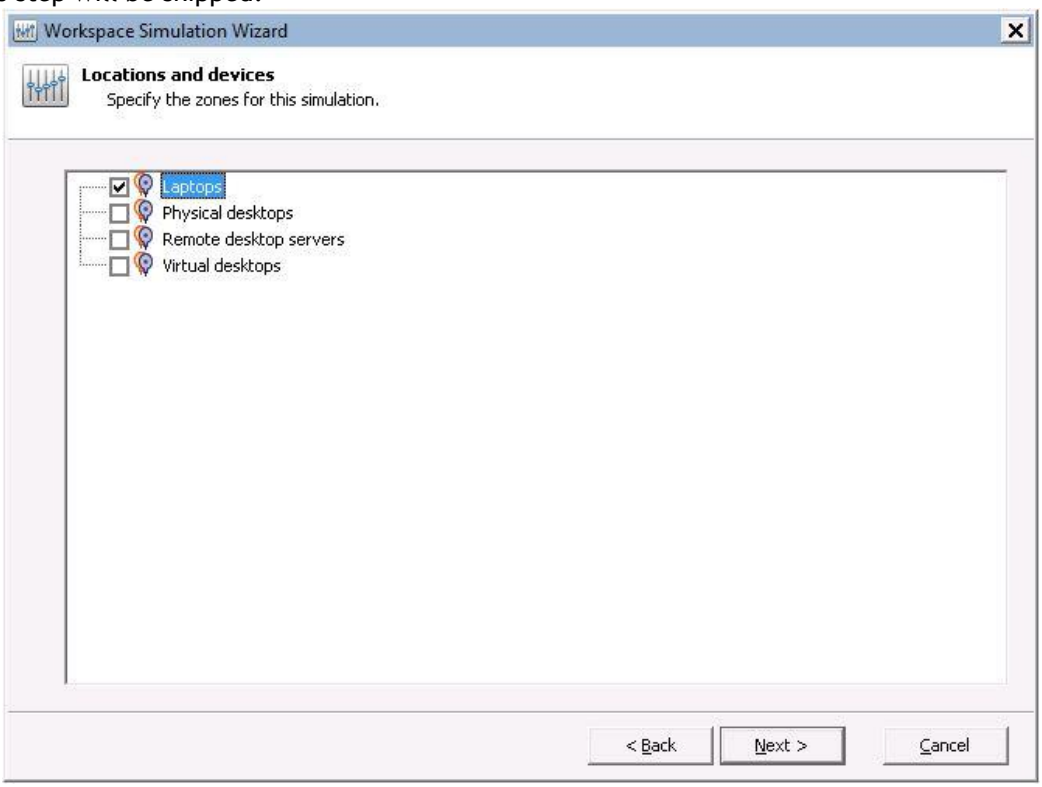
Creating a workspace simulation

1. When starting the workspace simulation wizard, an introductory window welcomes you to the wizard. Click **Next** to start.
2. If you start the wizard with a prefilled user identity, an existing user will already have been selected. If not, use the Browse buttons  to select users, OUs and/or groups. You can base the workspace simulation on:
   - **Existing users** from the Directory Service
   - **OU membership** or **Group membership**
     - You can **Search** for specific OUs or Groups by entering search criteria. You can use wildcards (e.g. "*team" will yield all OUs/groups containing "team").

- Click **Add manually** to select one or multiple Group(s) from the Directory Service. Multiple groups must be separated with semicolons and can be verified for existence by clicking **Check**.

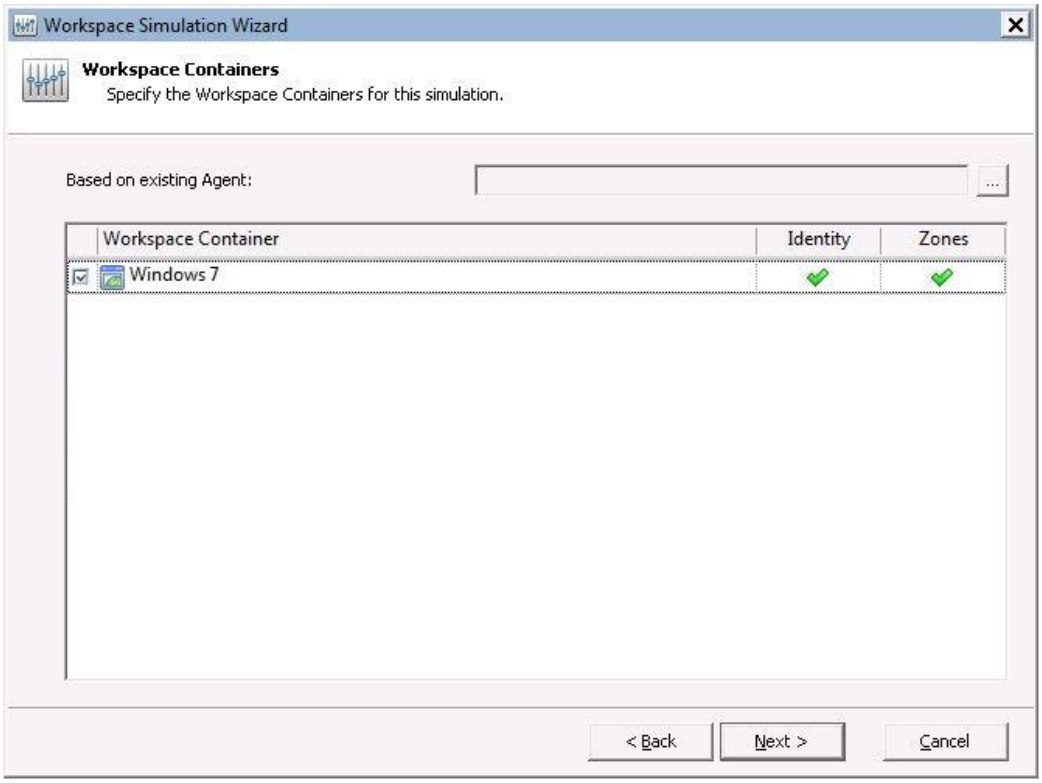


3. After selecting users, OUs and/or groups, click **Next**.
4. In the **Locations and devices** step, select one or more Zones. If no Zones have been configured, this step will be skipped.



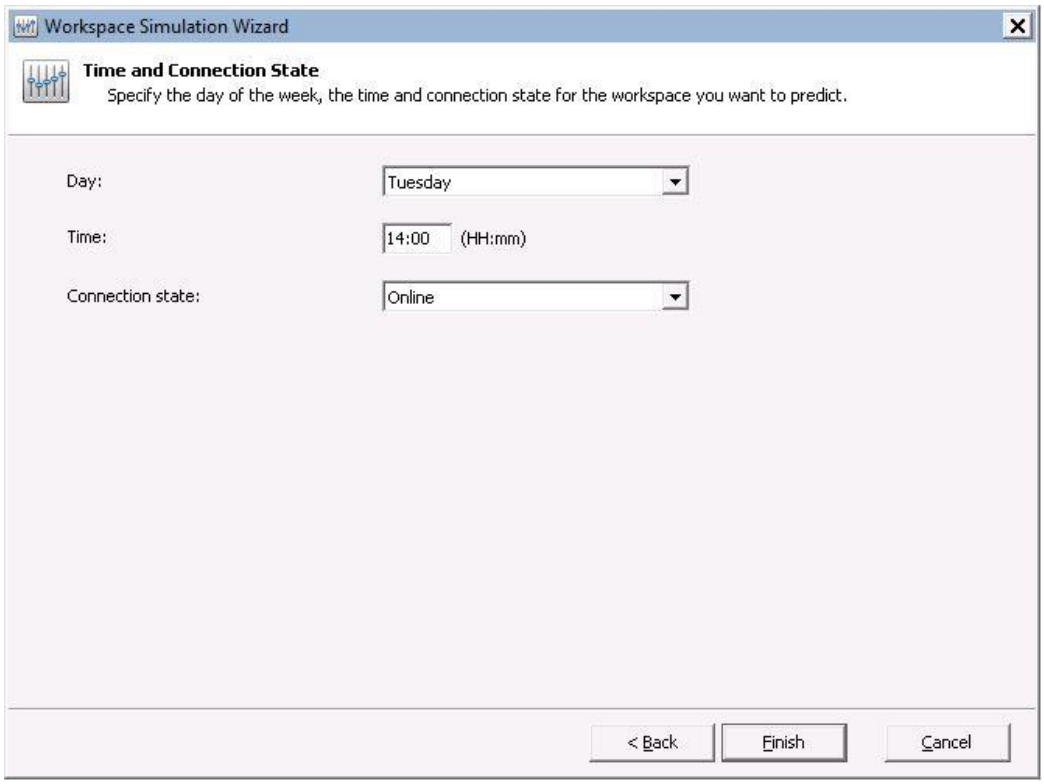
5. After selecting Zones, click **Next**.

6. In the **Workspace Containers** step, select one or more Workspace Containers. If no Workspace Containers have been configured, this step will be skipped. You can preselect the data based on an existing Agent (e.g. if the user logs on from a specific computer).



7. If the selected user's session will not be part of the selected Zone or available Workspace Container, the Wizard shows a red cross in an overview. This can be either an indication of an erroneous configuration, or a wrong scenario selection. All valid combinations of the user's identity with Zones and Workspace Containers show up with a green checkmark.
8. After selecting Zones, click **Next**.

9. In the **Time and Connection State** step, specify the day of the week, the time and connection state (Online/Offline) for the workspace you want to predict.



After specifying all criteria, the results of the Workspace Simulation are shown as if the predicted workspace was an actual workspace.

To create an Instant Report of the results, click **Action > Create Instant Report**. Save or print the report for later comparisons and analysis.

Example

You want to check whether a user can access a specific application from home and from work on a specific day/time.

You can run two simulations with the same user identity and an Online Connection state:

- Location A = Work, Workspace Container defines access on application level, day/time = e.g. Monday, 9:00
- Location B = Home, Workspace Container defines access on application level, day/time = e.g. Tuesday 9:00

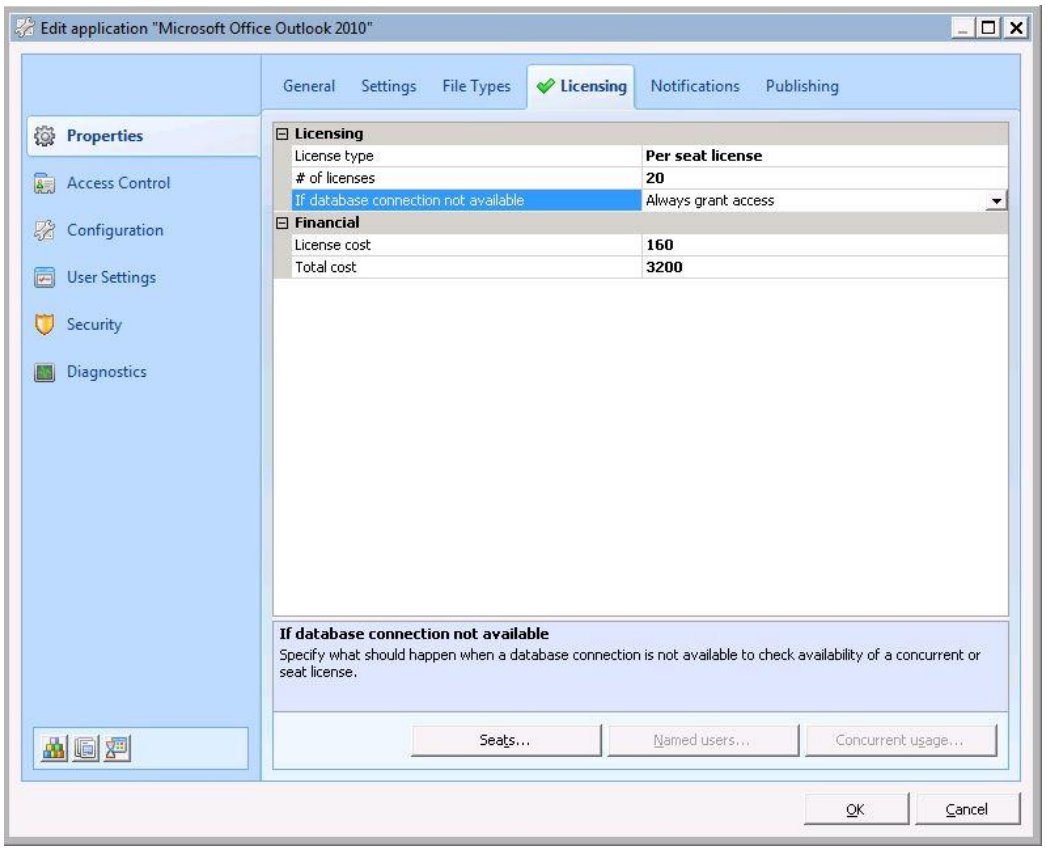
The result should be that the application is available from both locations and on both days and times

Note

A green check mark indicates that the criteria specified in the **Identity and/or Zones** step apply for this Workspace Container. A red cross indicates the criteria do not apply for this Workspace Container. This helps you to decide whether it is useful to include this Workspace Container in the scenario.

9.5 License metering

You can use the **Licensing** section of an application as a license metering tool, to manage the number of people that are allowed to use the application, based on the application licenses that are available. This allows you to force license compliance to e.g. Microsoft licensing models, while managing license usage in your RES Workspace Manager environment.



RES Workspace Manager supports the following application license types:

- **Company-wide license**: Grants unlimited access to all users in the RES Workspace Manager environment. The number of users can still be controlled through the Access Control options.
- **Server license**: Grants access to the application based on server licenses. If all server licenses are in use, additional users will not be granted access to the application. Instead, a message will be displayed that all licenses are in use.
- **Per seat license**: Seat licenses limit application usage to the number of computers that have logged in and claimed a seat. Click the **Seats** button to view the number of used seats and information about the computers (users) that have claimed them.

  With "Per Seat" licensing, it is possible to define a maximum number of seats per Zone. This can be used for example if each physical location within a company has a certain number of seat licenses available. In this case, define a Zone for each physical location, and set the maximum number of seats for each Zone. When seat licenses have been configured per Zone, the **View reserved and rejected seat licenses** window will let you choose which Zone to display the seat information for. To define the maximum number of seats per Zone, click the browse button ... next to the **# of licenses** field (this button will not appear until you have selected **Per seat license**). As long as there are no Zone-specific seats configured, RES Workspace Manager will work as before, with one global number of seat licenses.

- **Per named user license**: Grants access to the application based on specified users. This allows for back order situations, while keeping track of the actual available number of licenses. If all licenses are in use, additional users will not be granted access to the application. Instead, a message will be displayed that all licenses are in use. If application access is managed by an application manager, this message will be displayed to him.
- **Per concurrent user license**: Concurrent user licenses limit application usage to the number of concurrent users. This form of licensing is supported for local computing and centralized computing technology stacks. When all available licenses are in use, the next user who starts the application receives the message that all licenses are in use, plus a list of the users who are using the application at that moment. Users can resolve the distribution of licenses amongst themselves up to the total number of licenses.

Note

If you select **Per seat** licensing or **Per concurrent** licensing, the setting **Only RES Workspace Manager is allowed to launch this application** on the **Security section** will be selected automatically, to ensure that the user can only start the application via his Start menu or desktop. This allows RES Workspace Manager to check how many application licenses are in use.

Tip

Difference between # of licenses and # of users

The maximum number of users that can be granted access to an application can be set in the **# of users** field.

This is useful if you have granted users access while awaiting the arrival of extra licenses. For example: there are 100 licenses available and all licenses are already in use. You need to grant access to an additional 10 users that entered the company today. You can do this by setting the **# of users** field to 110 and order an additional 10 licenses. Until the licenses arrive, you can see the difference between the number of users and the actual number of available licenses, telling you that you have a back order running of 10 licenses or that you still need to buy 10 additional licenses. When the licenses arrive, you can then set the **# of licenses** field to the appropriate value, in this case 110.

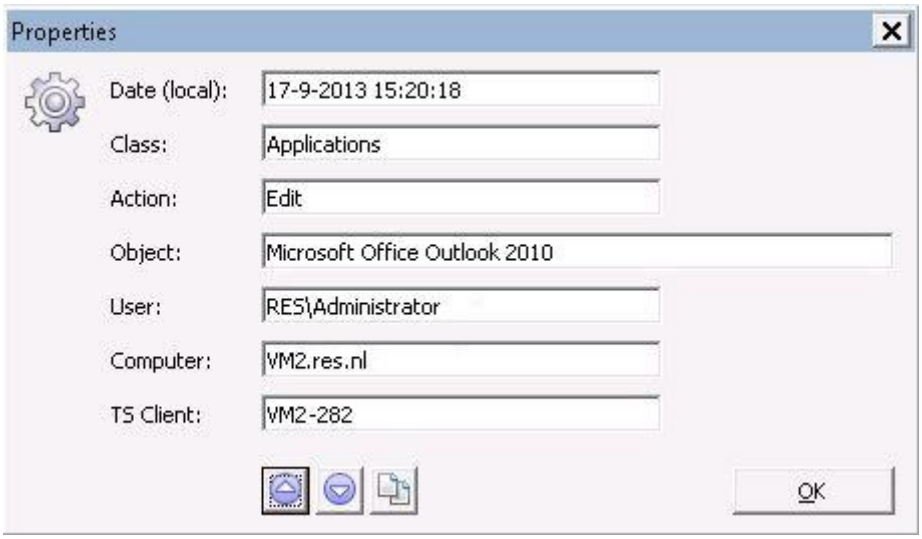
If an application uses Concurrent User licensing and the maximum number of users is reached on all Terminal Servers or workstations, the next user who starts up the application will receive a message that the maximum number of licenses has been reached. A list of concurrent users will also be displayed so that the user can take action without having to contact the IT department.

The Application Manager will see a similar message when he tries to grant a user access to an application for which the maximum number of available licenses has been reached.

9.6 Audit Trail

At **Diagnostics > Audit Trail** you can view display detailed information about all modifications in your RES Workspace Manager environment, including the installation of Service Packs (if applicable).

- To display the properties of an entry, right-click it and click **Properties**.



- To refresh the contents of the Audit Trail, click **Refresh**.
- To copy the contents of the Audit Trail to the clipboard, click **Copy**.
- To clear the Audit Trail log of all entries, click **Clear log**.
- To protect the **Clear log** button with a password, click **Security**. This will open the **Security** window, which allows you to enable password protection.
- If you already configured a password for the **Clear log** button, click **Security** to change this password. This will open the **Verify password** window. After entering the correct password, the **Security** window will open, which allows you to change the password.

Audit trails of single items

To display the **Audit Trail** window, select a node or window in the Console and click . For some items you can use the **Audit Trail** tab of an item. This will open the **Audit Trail** window, which allows you to view the audit trail of the selected object.

Chapter 10: Security & Performance

In this chapter we will deal with the subject of Security and Performance.

10.1 Security

Security restrictions in RES Workspace Manager help you secure the user workspace at different levels:

- **Applications**: prevents the use of unauthorized applications and executables.
- **Removable Disks**: secures the use of removable disks.
- **Files and Folders**: prevents the use of specific file types and folders.
- **Read-Only Blanketing**: renders all local drives on servers and desktops read-only.
- **Global Authorized Files**: allows you to authorize files, folders and drives.
- **Sessions**: restricts users to a single RES Workspace Manager session at a time.
- **Network**: prevents unauthorized network connections.

Except for security restrictions on network level, all security restrictions are based on a kernel mode driver (the AppGuard driver), which offers a high level of security while minimizing the overhead on your system. Security restrictions on network level are based on NetGuard, which is similar to AppGuard, but secures your network connectivity.

- System processes (such as `svchost.exe`) are also subject to Security. This means that these processes cannot start sub-processes (such as e.g. Windows Media Player or `.MP3` files) indirectly. **Global Authorized Files** (on page 218) contains a default rule that allows you to control this behavior.
- A Microsoft Windows Server console session is never protected by design.
- In general, if security restrictions are enabled, all executables that exist in the user's Start Menu are accessible to the user. All other executables are inaccessible.

10.1.1 Applications

Managed Applications

With security restrictions on **Applications**, you can prevent unauthorized applications and executables from being used in the user workspace. This prevents potentially harmful applications and executables from causing damage.

- Only applications that are made available to the user through RES Workspace Manager are authorized. All other applications are unauthorized, and are prevented from starting.
- Users are prevented from running executables that they received through e-mail or Internet. This prevents potentially dangerous executables containing viruses, spyware and malware from contaminating the corporate network.
- Users are prevented from using advanced commands in the command box.

Notes

- File types other than executables (for example .PDF, .DOC or .VBS) are accessible by default. You can block these file types (and folders) by configuring security restrictions on **Files and Folders**. See **Files and Folders security** (on page 215).
- Technical mangers are exempted from all Managed Applications security.

Applications security modes: disabled, learning, enabled

Global level

On global level, there are three modes for the security restrictions on **Applications**:

- In **disabled** mode, users can start applications and executables that are not managed by RES Workspace Manager and no data is logged.
- In **learning** mode, attempts to start unauthorized applications and executables will not be blocked, but can be logged. This helps you identify and authorize any executables that are started by authorized applications. When you have fine-tuned your environment sufficiently in **learning** mode, you can set Application security to **enabled** mode.
- In **enabled** mode, only authorized applications and executables can be started.

Notes

- If you select the option **Log security events**, security events will be logged if Applications security is in **enabled** or **learning** mode.
- If you select the option **Notify users about security events**, users will be notified if Applications security is in **enabled** or **learning** mode.

Application level

If you add a new application, it is not necessary to set Applications security to **learning** mode on global level, because this jeopardizes the existing security of the user workspace. Instead, it is sufficient to set only the new application to **learning** mode. The workspace remains secured, because only executables launched by the application will be allowed. Because these executables can be logged as a security event, this allows you to create application-specific exceptions.

If Applications security is enabled, the authorized files configured for a specific application will, by default, be enforced. You can configure authorized files for an application at **Managed Applications** on the application's **Security > Authorized Files** tab. See Authorizing files and folders.

Note

If the user is allowed to use the "cmd" command, any attempts to start executables will be blocked (e.g. a ping command). If necessary, you can authorize additional executables at application level.

Default behavior if running applications are no longer authorized

The availability of an application can be authorized, for example, on the basis of a Locations and Devices zone. Once an application is running in a user session, it can remain active if the user shuts down the computer without logging off from the session. Then, if the user logs on from another computer outside of the zone that authorized the application, the application may still remain active despite its lack of authorization. Similarly, the application may remain active even if the user is no longer a member of the Active Directory group that was the basis for the user's access to that application.

You can configure the default behavior for applications in such situations at **Security > Applications**.

- With the setting **If running application is no longer authorized, terminate application**, the application is terminated immediately (and abruptly) as soon a change in circumstances or configuration causes the user's authorization to disappear.
- If this is not necessary or desirable, for example because the application must be closed down correctly in order to prevent data loss, you can choose **If running application is no longer authorized, do nothing**.

To set different behavior for an individual application, open the application at **Composition > Applications** and change the setting on the tab **Security > Authorized Files**.

Managed Applications: Security section

The **security** section of a Managed Application determines the application's Files Security mode and authorized files; and its Network Security mode and authorized connections.

Authorized Files

Use the **Authorized Files** tab to configure specific security settings for an application.

When a user starts an application, the application usually needs to access other files and executables to function properly. Access to certain files and folders can be blocked on a global level at **Security > Data > Files and Folders**. If a certain application needs a file or folder that is blocked on a global level, you could authorize these files and executables on a global level, but this may be undesirable. The alternative approach is to authorize the necessary files and folders for the specific application only. This approach provides the best protection of the user workspace.

- Global authorized files are configured at **Security > Global Authorized Files**.
- Application authorized files are configured at **Managed Applications** on the application's **Security** tab.

Configuration

- To add, edit or remove authorized files and folders for a specific application, open the application at **Managed Applications** and go to **Security > Authorized Files**.
- Select **Run this application in learning mode** if all access to files and folders by this application should be allowed but also logged. Run an application in learning mode for a while to find out which files and executables should be authorized for the application
- To ensure that a user can only start the application in his RES Workspace Manager session, select **Only RES Workspace Manager is allowed to launch this application**. This ensures that a user can only use his Start Menu or desktop to start the application, and not e.g. a command prompt or Windows Explorer. This is useful if you want to force license compliance in your organization, because it allows RES Workspace Manager to determine the actual number of application licenses in use. This setting is also useful if certain settings for the application are indispensable (e.g. registry settings). In the following situations, this setting is selected automatically and grayed out:
- When using concurrent or seat licenses (See **Licensing** on page 98) for the application.
- When adjusting the process priority of the application on the **Settings** tab.
- The default value for the setting **If running application is no longer authorized** is configured at **Security > Applications**. You can change the behavior of the current application so that it does not follow the default anymore.
- You can authorize files and executables by adding a file or executable to the list of authorized files, but you can also authorize a file or executable directly from the log:
- Click the **Log** tab. This shows an overview of security events that were caused by the application.
- Select the file or executable that caused the security event and click **Authorize selected incident**. This will open the **Authorize file** window. The **Authorized File** field will be populated with the values of the incident that you selected.
- Changes on the **Authorized Files** tab will not come in effect until you click **OK** and close the **Edit application** window.

Tips

- You can easily move authorized files from one application to another; from an application to the global Authorized Files node; and from the global Authorized Files node to a specific application. To do so, right-click one or more selected authorized files and choose Move.
- On the **Applications List** tab of the **Managed Applications** node, the column **Learning mode** shows whether an application is set in learning mode or not.

Example:

The availability of an application can be authorized on the basis of a Zone. Once an application is running in a RES Workspace Manager session, it can remain active if the user shuts down the computer without logging off from the session. Then, if the user logs on from another computer outside of the Zone that authorized the application, the application may still remain active despite its lack of authorization.

This breach of authorization can be prevented with the setting **If running application is no longer authorized, [terminate application]**.

If this is not necessary, RES Workspace Manager can also be configured with **If running application is no longer authorized, [do nothing]**.

The default for this setting is configured at **Security** > **Applications**. Different behavior can be set for individual applications by opening the application at **Composition > Applications** and changing the setting at **Security > Authorized Files**.

Authorized Connections

Use the **Authorized Connections** tab in an application's **Security** section to allow the application to use network connections that are blocked through the Network Security configured at **Security > Network**. This may be necessary for database applications, ICA/RDP clients, telnet applications, SSH clients, MSN Messenger, etc.

Configuration

- If you need to determine which network connections should be authorized for the application, but you do not want to disable global Network Security, select **Run this application in learning mode**. In learning mode, the application can still access unauthorized network connections, but these are logged.
- To convert a **Log** entry to an Authorized Connection, select the network connection that was logged as a security event, and click **Authorize selected incident**.

Note

A rule authorizing a Network Connection at application level overrules a rule blocking that same connection at a global level.

Tip

You can easily move authorized connections from one application to another; from an application to the global node Network; and from the global Network node to a specific application. To do so, right-click one or more selected authorized connections and choose Move.

Dynamic Privileges

Use the **Dynamic Privileges** tab to elevate or restrict rights for applications while maintaining default privileges for the user. This allows you to grant administrative privileges to specific applications that need these privileges (such as proprietary applications, Control Panel applets (using `rundll32.exe` or `control.exe)` and applications that allow changes to be made to hardware settings) without granting the user full rights as an administrator. Reducing user privileges may be useful for granting a user that is an administrator an application that should not be run as an administrator, such as a command prompt.

Configuration

Access token:

- **Do nothing** (default) - Does not change any rights for this application.
- **Add administrator rights** - Forces the application to be started with administrator rights.
- **Remove administrator rights** - Forces the application to be started without administrator rights.

Example:

To make a Control Panel applet available create a new application in the RES Workspace Manager Console with `%systemroot%\windows\rundll32.exe` and the appropriate parameter. Add administrator rights to the applet using Dynamic Privileges. For instance:

Date & Time Properties	
Module	TIMEDATE.CPL
Command:	`rundll32.exe shell32.dll,Control_RunDLL timedate.cpl,,0`
result:	Displays Set Date & Time properties tab
Command:	`rundll32.exe shell32.dll,Control_RunDLL timedate.cpl,,1`
result:	Displays the Time Zone properties tab

See Making Control Panel Applets (CPL files) available as applications for a more extensive list of Control Panel applets and their command lines.

Logging

All Applications security events are logged in the **Applications Log**. This log shows an overview of all events that occurred when users were prevented from starting an unauthorized executable. The log is automatically cleaned up periodically.

Many applications need to start up other, legitimate executables in order to function properly. For example, some application Help features will call on an executable. If that executable is blocked, the user cannot access the Help. You can allow these specific executables to run in your environment by authorizing them from the **Applications Log**. These specific executables will be set as **Global Authorized Files**.

User Installed Applications

User Installed Applications give users the right to install software on specific computers. This can be particularly useful to give expert users a degree of control over their own computer, so that they can install software themselves as and when needed. User Installed Applications are always restricted to specific computers, based on Workspace Containers and/or Zones, and can optionally be further restricted to specific users.

For example, a department may be in the process of developing a new application. They receive new versions several times a week, and each version needs to be installed before it can be tested. It is extremely inefficient for the administrator to have to do this each time. Instead, you can enable User Installed Applications with **Access Control** set to specific people in that department, and **Workspace Control** set to a Workspace Container that holds the computers in that department. As a result, the specified users can install the updates on the specified computers.

Similarly, a small number of people might use a highly specialized software package such as AutoCAD. They may well know more about the software than the administrator does, and so it makes more sense to allow them to install the AutoCAD updates or extensions themselves.

Users who are allowed to install User Installed Applications on a computer, get an extra tab in their "Workspace Preferences" tool, from which they can install software using a wizard. With this wizard, they can create shortcuts for these applications in their Start menu, on their Desktop, on their Quick Launch bar and in their Startup items.

Configuring User Installed Applications

- There are three modes in which the User Installed Applications functionality can run (configured on the **Settings** tab):
- **Allow any setup to run** - Any application may be installed by the user if the user has local administrator rights.
- **Blacklisting** - *Any* application may be installed by the user, except applications that comply with a set **Deny** rule. Note that by using Access Control and Workspace Control it is possible to set a global **Deny** rule in combination with a specific **Allow** rule (e.g. Deny all software installations by a specific Publisher, but allow this for a specific Group). All Deny rules are checked for a possible match, if a match is found then all Allow rules are checked for possible exception. If no match is found, the user is notified that this setup is not allowed.
- **Whitelisting** - *No* applications may be installed, except applications that comply with a set **Allow** rule. Note that by using Access Control and Workspace Control it is possible to set a global **Allow** rule in combination with a specific **Deny** rule (e.g. Allow all software installations by a specific Publisher, but deny this for a specific Group). All Allow rules are checked for a possible match, if a match is found then all Deny rules are checked for possible exception. If a match is found to a Deny rule, the user is notified that this setup is not allowed.

Note

In case Administrative Roles are used (at **Administration > Administrative Roles**), making changes to the setting **Software installations** is only permitted by Administrative Roles that have **Modify** access to the **Security > Applications > User Installed Applications > Settings** tab (on the **Settings** tab of the Administrative Role).

- User Installed Application Rules (i.e. **Allow** and **Deny** rules) can be based on:
- **Publisher in signature**
- **Product name in file properties** (only in combination with Publisher)
- **Product version in file properties** (only in combination with Publisher)
- **Checksum of file** (only if no other criteria are selected)
- These values can be entered manually or by browsing to a specific installation file. Note that wildcards are allowed.
- To give a user temporary local administrator rights when installing specified applications, the **Software installations** mode **Whitelisting** and **Run installation using Dynamic Privileges** may be selected. See Dynamic Privileges.

User Installed Applications must always be restricted to specific computers in a Workspace Container or in a Zone. Although you can combine several Workspace Containers and/or Zones, the minimum requirement is one Workspace Container or one Zone.

- Specify the Workspace Container(s) on the **Workspace Control** tab.
- Specify the Zone(s) on the **Access Control** tab under **Location**.
- Optionally, you can restrict the right to install User Installed Applications on the specified computers to specific OUs, groups, users, administrative roles and RES IT Store Services. You can specify this on the **Access Control** tab under **Identity**.

The **Log** tab shows who installed or removed what unmanaged applications on which computers.

- You can sort columns by clicking on the column headers. Columns can be moved and resized by dragging and dropping the column headers. In the **Options** menu, the option **Reset all column properties to defaults** can be used to restore the columns to their original position and size.
- To filter the view by computer name, select the computer from the **Computer** drop-down list.
- In the filtered view, click  for a list of User Installed Applications on the selected computer.

Warning

Users who are allowed to install User Installed Applications on a computer can choose to install any application they like. However, what they install can be monitored (at **Security > Applications > User Installed Applications** on the **Log** tab).

Notes

- User Installed Applications do not become available in the **Managed Applications** node of the Management Console.
- A user can only install unmanaged software if he has the appropriate local privileges to install new software.
- By design, User Installed Applications cannot be installed on Terminal Servers, even if the user session on the Terminal Server complies with all the criteria set for User Installed Applications.

Websites

At **Security > Websites** , you can enable user specific website filtering based on rules.

There are two methods for using Website Security:

- **Whitelisting** means specific URLs are allowed and all others are denied.
- **Blacklisting** means that specific URLs are denied and all others are allowed.

For fine-tuning purposes, exceptions to the set rules can be made.

Website filtering is done by WebGuardIE, an add-on for Microsoft Internet Explorer.

Note

In case Administrative Roles are used (at **Administration > Administrative Roles**), making changes to the setting **Security method** is only permitted by Administrative Roles that have **Modify** access to the **Security > Applications > Websites > Settings** tab (on the **Settings** tab of the Administrative Role).

Configuring Website Security

- On the **Websites** tab you may enter **allow** or **deny** rules for websites, depending on the method used (configured on the **Settings** tab).
- Rules may contain an '*'. The asterisks are regarded as wildcards. If an IP address is entered as URL, WebGuard will try to resolve the IP address and the resulting URL will be checked. Rules can be entered without `http://`, `https://` or other prefixes.
- **Blacklisting** *allows* all Websites, except the ones listed, the so-called "Blacklist". Entering only allow rules therefore, has no effect (hence the default is **Deny**). Allow rules are exceptions to the deny rules. An URL is first checked against the deny rules. When the URL passes this check, i.e. there is no deny rule for this URL, the web page will be displayed. When an URL has a deny rule hit, the URL will be checked against the allow rules. When the URL does match an allow rule, the web page will be displayed despite the matching deny rule. The allow rules are used as exceptions to the deny rules and can be used for fine tuning RES WebGuardIE.
- **Whitelisting** *denies* all Websites, except the ones listed, the so-called "Whitelist". Entering only deny rules, therefore, has no effect (hence the default is **Allow**). Deny rules are exceptions to the allow rules. An URL is first checked against the allow rules. When the URL does pass this check, i.e. there is an allow rule matching the URL, the URL will then be checked against the deny rules. When the URL has a deny rule match, the web page will not be shown, despite the matching allow rule. The deny rules are used as exceptions to the allow rules and can be used for fine tuning RES WebGuardIE.
- You can configure exceptions to Website Security, to give specific users on specific locations specific permissions.
- If necessary, you can authorize websites that caused a security event on the **Log** tab.
- On the **Log** tab, it is possible to export the log entries to a `.csv` file.
- On the **Settings** tab, enabling **Log all visited websites** for security events, will result in all visited whitelisted/allowed websites having the value ALLOW in the Action column on the **Log** tab, and blacklisted/denied websites the value BLOCK.
  Please note that enabling this option may produce quite some extra logging in the Datastore.
- Click **Message** to configure security notifications that will be shown if a Removable Disks Security event occurs (**Settings** tab).
- You can override the global settings of this feature for specific Workspace Containers.

Notes

- To prevent users from circumventing the applied rules, the following policies are automatically set:
  - **inPrivate browsing**. Internet Explorer 8.0 supports InPrivate browsing mode. When using InPrivate browsing mode, Helper Browser Objects are not active. In order to prevent users from circumventing WebGuard, the InPrivate mode is disabled. This registry setting can be found at: `HKCU\Software\Policies\Microsoft\Internet Explorer\Privacy REG_DWORD EnableInPrivateBrowsing`
  - **Protected Mode** in Microsoft Internet Explorer 8.0 and higher on Windows 7 / 2008 should be disabled. This setting is enabled by default. This policy can be found at `\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone` and is by default available in `inetres.admx` on Microsoft Windows 7 / 2008 systems.
  - **NoExtensionManagement**. Users should not be able to disable WebGuard. To prevent users from disabling WebGuard the **NoExtensionManagement** registry setting is set. This registry setting can be found at: `HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions REG_DWORD NoExtensionManagement`
- Prerequisites: Microsoft .NET framework version 2.0 SP2; 32-bit Internet Explorer 6.0 or higher.
- The option **Log all visited websites** for security events is supported for Microsoft Internet Explorer 8, 9, and 10.

Examples

Blacklisting examples

The following rules are set:

- `*.com` - deny
- `news.cnet.com` - allow

Result:
All `.com` URLs are denied except `news.cnet.com`

The following rules are set:

- `company.*` - deny
- `company.de` - allow

Result:
All `company` URLs are denied except `company.de`

Whitelisting example

The following rules are set:

- `*.com` - allow
- `news.cnet.com` - deny

Result:
All `.com` URLs are allowed except `news.cnet.com`

Whitelisting example

The following rules are set:

- `*.google.com` - deny
- `Maps.*.com` - allow

In Whitelisting mode URL `http://maps.google.com` will be denied, in Blacklisting mode it will be allowed.

10.1.2 Data

Removable Disks security

With security restrictions on **Removable Disks**, you can secure the use of removable disks in the user workspace by giving only specific users on specific locations specific permissions to use removable disks. This allows you to increase the security of your organization by preventing unauthorized users from, for example, copying sensitive corporate data to and from floppy disks, DVD/CD disks, USB sticks, FireWire drives, etc, or accidentally infecting the system network with viruses and other malware. Other removable media, such as mobile phones, PDAs and CD/DVD burners, can only connect to a computer using specific software, which you can manage with Managed Applications.

Notes

- Access to DVD/CD writing functionality is often managed through application access and not by Removable Disks security. Standard DVD/CD writing functionality of the operating system (as present in Microsoft Windows XP and Vista, for example) is managed by Removable Disks Security.
- USB 3.0 hubs are supported for Removable Disk Security.

Removable Disks security modes: disabled, learning, enabled

There are three modes for the security restrictions on Removable Disks:

- In **disabled** mode, users can access any removable storage device and no data is logged.
- In **learning** mode, any user actions will not be blocked, but can be logged. When you have fine-tuned your environment sufficiently in **learning** mode, you can set Removable Disks security to **enabled** mode.
- In **enabled** mode, only authorized removable storage devices can be accessed.

Notes

- If you select the option **Log security events**, security events will also be logged if Removable Disks Security is in **learning** mode.
- If you select the option **Audit allowed write actions**, allowed write actions will also be logged if Removable Disks Security is in **learning** mode.
- If you select the option **Notify users about security events**, users will also be notified if Removable Disks Security is in **learning** mode.

Assigning permissions to users

You can give specific users on specific locations specific permissions to use removable storage devices.

Permissions

You can assign different permissions (**Read** and/or **Modify**) to floppy disks, dvd/cd disks and removable disks (e.g. you can assign **Modify** permissions to floppy disks, **Read** permissions to dvd/cd disks, and no permissions to removable disks).

Files and folders on removable storage devices are not blocked according to the security restrictions on **Files and Folders**:

- A user with **Modify** permissions on a removable storage device can always delete, copy, move and rename the files and folders on that device.
- If certain file types are blocked by the security restrictions on **Files and Folders**, files of this type on the removable storage device cannot be opened *unless* they have been authorized. You can authorize these files either on global level (from the **Log** tab or from **Security > Global Authorized Files**) or on application level (at **Managed Applications** on an application's **Security > Authorized Files** tab). A blocked file can neither be copied or moved from the removable storage device to other locations. See Authorizing files and folders.

Access Control and Workspace Control

By combining Access Control criteria and Workspace Control criteria, you can create situations where an authorized user can only access a removable storage device at an authorized location on an authorized computer.

Drive mappings

If a removable storage device is mapped to a drive, Microsoft Windows remembers this mapping and will try to use it again next time the removable storage device is used. If that drive letter is no longer available, the removable storage device does not become visible. To prevent this, select **Map Removable Disk to first available drive letter starting from** and provide the drive letter of your preference. If you enable this option, RES Workspace Manager will first try to map the drive to the preferred letter. If this is not available, it will proceed alphabetically until a free letter is found. After Z, it will start at A.

Logging

All Removable Disks security events are logged in the **Removable Disks Log**. This log shows an overview of all events that occurred when users were prevented from accessing a removable storage device. The list specifies time, file name and location, process, computer, user, session, operation, and action. The log is automatically cleaned up periodically.

You can authorize a blocked file from the **Removable Disks Log** by selecting it and clicking **Authorize selected file**. This exception can be **Execute** and/or **Modify**. Alternatively, you can authorize the file by right-clicking it and then selecting **Authorize selected file** from the context menu. It will then automatically be added to the **Global Authorized Files**.

Files and Folders security

With security restrictions on **Files and Folders**, you can prevent specific file types and folders (such as *.vbs, *.avi, or \\server\share\folder*) from being used in the user workspace.

Files and Folders security Mode: disabled, learning, enabled

There are three modes for the security restrictions on Files and Folders:

- In **disabled** mode, users can use any file or folder and no data is logged.
- In **learning** mode, attempts to use unauthorized files and folders will not be blocked. However, you can choose to log these events in the **Log** file. This allows you to fine-tune the security of your environment by authorizing additional files, if necessary. When you have fine-tuned your environment sufficiently in **learning** mode, you can set Files and Folders security to **enabled** mode.
- In **enabled** mode, unauthorized files and folders cannot be accessed. You can choose to log security events in the **Log** file.

Notes

- If you select the option **Log security events**, security events will also be logged if Files and Folders security is in **learning** mode.
- If you select the option **Notify users about security events**, users will also be notified if Files and Folders security is in **learning** mode.
- If you configure a blocked resource type, **Silent** mode on the **Settings** tab will block the resource, but not log a security event. This can be useful if the resource causes many security events, and you want to filter these events from the **Files and Folders Log**.

Example: blocking and authorizing files

With Files and Folders security, you can set up a situation in which certain files are blocked for general use, but can be accessed by a specific application.

For example:

- .MP3 files and .AVI files should be blocked for all users.
- Only managers should be allowed to access .MP3 files and only when using Windows Media Player.

This setup can be achieved with the following:

1. Configure blocked resources in Files and Folders security for the file types `*.mp3` and `*.avi`.
2. Add the application Windows Media Player in the **Managed Applications** node.
3. In the **Access Control** section of the application window, add **Management** to the list of selected groups.
4. In the **Security** section, select **Only RES Workspace Manager is allowed to launch this application**.
5. Add an authorized file for the file type `*.mp3`.

Logging

All Files and Folders Security events are logged in the **Files and Folders Log**. This log shows an overview of all events that occurred when users were prevented from accessing an unauthorized file or folder. The list specifies time, file, process, computer, user, session, operation and action. Use the drop-down box in the lower part of the screen to sort events by date. The log is automatically cleaned up periodically.

You can authorize a blocked file from the **Files and Folders Log** by selecting it and clicking **Authorize selected file**. It will then automatically be added to the **Global Authorized Files**, and access to it will no longer be prevented.

Read-Only Blanketing

With **Read-Only Blanketing**, you can render all local drives on servers and desktops in your environment read-only, without touching Microsoft Windows security permissions on files and folders. This allows you to safeguard data against unauthorized access or modification by RES Workspace Manager users, and secures the user workspace against corruption and loss of information.

Read-Only Blanketing allows you to prevent users from:

- Saving data on local drives. If Read-Only Blanketing is enabled, data can only be saved on network drives.
- Accidentally overwriting or deleting system files and other important files on their desktops.

The following folders are automatically excluded from Read-Only Blanketing:

- The Recycle Bin on each local drive
- %userprofile%, %allusersprofile%
- Tmp and temp locations
- Spool in system32 folder
- Debug\usermode in system32 folder
- The server console

Read-Only Blanketing security Modes: disabled, learning, enabled

There are three modes Read-Only Blanketing:

- In **disabled** mode, users can access and modify data on local disks and no data is logged.
- In **learning** mode, attempts to access local disks will not be blocked. However, you can choose to log these events in the **Log** file. When you have fine-tuned your environment sufficiently in **learning** mode, you can set Read-Only Blanketing to **enabled** mode.
- In **enabled** mode, all local drives on servers and desktops are rendered read-only. You can choose to log security events in the **Log** file.

Notes

- If you select the option **Log security events**, security events will also be logged if Read-Only Blanketing is in **learning** mode.
- If you select the option **Notify users about security events**, users will also be notified if Read-Only Blanketing is in **learning** mode.

Logging

All Read-Only Blanketing security events are logged in the **Read-Only Blanketing Log**. This log shows an overview of all events that occurred when users were prevented from accessing an unauthorized file or folder. The list specifies time, file, process, computer, user, session, operation and action. Use the drop-down box in the lower part of the screen to sort events by date. The log is automatically cleaned up periodically.

You can authorize a blocked file from the **Read-Only Blanketing Log** by selecting it and clicking **Authorize selected file**. Alternatively, you can authorize the file by right-clicking it and then selecting **Authorize selected file** from the context menu. It will then automatically be added to the **Global Authorized Files**, and access to it will no longer be prevented.

10.1.3 Authorized Files

With **Authorized Files**, you can authorize files and folders in the user workspace, and view a list of all authorized files. Files and folders that are authorized on global level can be accessed by all users, but you can still maintain a high level of security in the user workspace by applying Access Control criteria and Workspace Control criteria to each global authorized file.

Before you authorize a file on global level, always consider if the user workspace is better protected if you authorize the file on application level.

Authorizing files and folders

You can make exceptions to the global blocking of files by authorizing access to specific files and folders. Authorization can be global, or it can be provided on an application level.

- Grant global access to specific files either through the **Authorized Files** section, or by authorizing files from the various security logs.
- Many applications need to start up other, legitimate executables or to access specific files in order to function properly. For example, some application Help features will call on an executable. If that executable is blocked, the user cannot access the Help. You could authorize these files and executables on a global level, but this may be undesirable. Instead, you can grant a specific application (rather than all users) the right to access a specific file. This application is then allowed to access the file, but other applications or users are not. You can set access to a file for an application on the tab **Security > Authorized Files** for the specific application.
- With the security restrictions on **Files and Folders**, you can block certain file types. You can still authorize individual files of this type on global level (**Security > Authorized Files**) or on application level (at **Managed Applications** on an application's **Security > Authorized Files** tab).
- You can easily move authorized files from one application to another; from an application to the **Authorized Files** node; and from the **Authorized Files** node to a specific application. To do so, right-click one or more selected authorized files and choose **Move**.

When adding an authorized file or folder to the Global Authorized Files, use the following formats:

Format	Explanation
`C:\WINDOWS\inf`	File or folder with this name
`C:\WINDOWS\inf\`	Only this folder
`C:\WINDOWS\inf\*`	All files and subfolders in folder `C:\WINDOWS\inf`
`C:\WINDOWS\inf\*.txt`	All files with the extension .txt in folder `C:\Windows\inf`
`C:\WINDOWS\inf\readme.txt`	Only the file Readme.txt in folder `C:\Windows\inf`

Note

Authorized Files contains a default rule for the system process `svchost.exe`. In some operating systems, this process causes applications to start when double-clicking a file that is associated with it, even when the application is blocked by a security rule. This security rule determines whether `svchost.exe` is allowed to start other unmanaged applications or file associations (such as e.g. Windows Media Player and `.MP3` files) indirectly. In new RES Workspace Manager environments, the rule is **disabled** by default. In environments that are upgraded from a previous version of RES Workspace Manager, the rule is **enabled** by default.

10.1.4 User Sessions security

With the security restrictions on **User Sessions**, you can restrict users to a single RES Workspace Manager session at a time. This improves the performance of your application servers and allows you to manage license usage. It also prevents issues with locked data in a user's home folder, which sometimes occurs when a user tries to access the same data from two sessions simultaneously.

When users try to start a second RES Workspace Manager session, a message shows that they already have an active session, and are not allowed another session. This message can be configured.

- **Allow end users to log on more than once from the same workstation** allows the user to start different applications that are located at different Terminal Servers in the same RES Workspace Manager session. For example, this allows the user to start Microsoft Office at Terminal Server A and a financial application at Terminal Server B in the same RES Workspace Manager session.
- If the option **Allow end users to end/disconnect an already active session** is enabled, end users can end the previous session and proceed with the logon in the second location. If the option **Show list of applications in the already active session** is enabled, they can see which applications are still open in the active session. This can be useful, because any unsaved data in the active session will be lost.

Configuring different settings for certain parts of the environment

The security restrictions on **Sessions** apply to the entire RES Workspace Manager environment. However, in certain situations you may want certain parts of the environment to get different settings.

Excluding certain types of users

There are two options to exclude users from the default security restrictions on **Sessions** on the basis of an Administrative role. This can be useful, for example, for a system administrator that needs to be able to log on at multiple machines, without being hindered by the security restrictions on **Sessions**.

- With **Allow any user with assigned Administrative Role to log on more than once**, users with an Administrative Role are excluded from the security restrictions on **Sessions**, and can start several sessions. This applies to any user who has an Administrative Role, whatever that Administrative Role is.
- With **Allow technical managers to log on more than once**, users who have the Administrative Role of Technical Manager are excluded from the security restrictions on **Sessions**. Users with other Administrative Roles are not excluded from the security restrictions on **Sessions**.

Excluding passthrough sessions

Passthrough sessions are sessions that occur when a user starts an application that is located on a remote server from his RES Workspace Manager session. When the user starts the application, a new session is started on the remote server to deliver the application to the user's desktop. This can be a Citrix XenApp published application or a Microsoft TS RemoteApp applications. With the option **Always allow passthrough sessions**, you can exclude these sessions from the security restrictions on **Sessions**.

You can read more about Citrix XenApp published applications and Microsoft TS RemoteApp applications in the chapter Integration.

Logging

All Sessions Security events are logged in the **Sessions Log**. This log shows an overview of all events that occurred when users were prevented from starting a new session. The log also shows which action was taken by the user:

- **Exited on user request**.
- **Retried** (if the user logged off the other session manually, and then retried).
- **Logged off other session on client 'clientname'** (if the user opted to let RES Workspace Manager log off the other session automatically).

The log is automatically cleaned up periodically.

10.1.5 Network Connections security

With the security restrictions on **Network Connections**, you can restrict access to resources on the network per user workspace.

Network Connections security can be configured for the entire user session, or for specific applications assigned to the user.

Agent Prerequisites

In order to use Network Security, Agents must be running one of the following operating systems (including the 64-bit editions):

- Microsoft Windows 2000 SP4 with Update Rollup 1.
- Microsoft Windows XP SP2
- Microsoft Windows Vista
- Microsoft Windows Server 2003 SP1
- Microsoft Windows Server 2008
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1

If you enable Network Security while your computer (the administrator's computer) does not meet the prerequisites, a message will show that the NetGuard driver is not found or is not running.

If Network Security is enabled, users will not be able to start sessions on Agents that do not meet the requirements. To allow users to start sessions on such Agents anyway, select **Allow session on computers not running NetGuard**.

Network Security Modes: disabled, learning, enabled

Global level

There are three modes for the global settings of the Network Security feature:

- In **disabled** mode, Network Security allows all network connections, and no data is logged.
- In **learning** mode, Network Security allows all network connections. However, you can choose to log these events. Use learning mode to monitor and evaluate which network connections are used without restricting users in their work.
- In **enabled** mode, Network Security is enforced: authorized network connections are allowed and unauthorized connections are blocked. You can choose to log attempts to access blocked connections.

Notes

- If you select the option **Log security events**, security events will be logged if Network security is in **enabled** or **learning** mode.
- If you select the option **Notify users about security events**, users will be notified if Network security is in **enabled** or **learning** mode.

Application level

If Network Security is enabled or in learning mode, all of the configured Authorized Connections will be enforced to all applications. If you need to determine which network connections should be authorized for an application, you can run this application's Authorized Connections in learning mode so that it can still access unauthorized network connections, but these are logged.

Individual blocked connections

If Network Security is enabled or in learning mode, a new blocked connection is set in learning mode by default. This allows you to monitor the use of this connection, which will be allowed but also logged. If the connection should indeed be blocked, the rule must be set in blocking mode.

Security Method: Whitelisting or Blacklisting

The global Network Security feature has two Security Methods: Whitelisting and Blacklisting.

- **Whitelisting** allows *no* network connections, except the ones that are listed on the **Authorized Connections** tab.

  Whitelisting gives you full control over the network connections in your environment. Only authorized connections can be accessed. However, for this approach to work, you do need to know exactly which network connections are required in your environment, so that you can authorize them. If you find out someone is trying to access a new network connection that should be allowed, you add that connection to the list of authorized connections. Optionally, Access Control and Workspace Control can authorize the connection only for certain people or workspaces.
- **Blacklisting** allows *all* network connections, except the ones that are listed on the **Blocked Connections** tab.

  Blacklisting allows you to block network connections that you do not want users to access. Blocked connections cannot be accessed, all others can. If you find out people are accessing a new network connection that you do not want them to, you add that connection to the list of blocked connections. Optionally, use Access Control and Workspace Control to block the connection for certain people or workspaces.

Exceptions to blocked connections when Blacklisting

With Blacklisting, you can create an exception so that certain people, workspaces or processes can access a connection that is blocked for others:

- To allow a process to access a connection that is blocked on the global level, authorize the connection on the application's **Authorized Connections** tab.
- To allow certain people and/or workspaces to access a connection that is blocked on the global level, create an Authorized Connection on the **Authorized Connections** tab at **Security > Network**. Access Control and Workspace Control on this Authorized Connection must result in a subset of the people and/or workspaces that the global blocked connection applied to.

Creating a Blocked Connection for monitoring purposes in Blacklisting environments

If Network Security is enabled and uses Blacklisting, you can monitor what connections are actually established by setting up a special blocked connection in learning mode. This blocked connection for monitoring purposes ensures that all connections that are not blocked are logged.

To create a blocked connection for monitoring purposes, create a blocked connection with a wild card (*) in all the fields, and set it in learning mode. Ensure that the blocked connection appears at the very bottom of the list of blocked connections.

Global Network Security and application-based Authorized Connections

Authorizing a specific application to use specific connections

Exempting an application from Network Security Settings

Authorizing a specific application to use specific connections

- With Network Security enabled and using Blacklisting, use an application-level Authorized Connection to overrule a blocked connection at the global Network Security level.
- With Network Security enabled and using Whitelisting, use an application-level Authorized Connection to add an additional layer of security: the connection is authorized, but only for the application process. The connection cannot be accessed from another application. For example, if you authorize connection to a specific server group by an SSH Client application, the connection will only be available if it is accessed from the SSH Client. If any other application or process attempts to set up that connection, Network Security will block or log it, depending on its configuration.

Exempting an application from Network Security Settings

To exempt an application from Network Security settings as configured at **Security > Network**, select **Run this application in learning mode**. This allows the application to access all network connections, whether they are blocked or not. In learning mode, these network connections are logged.

This setting is useful if you need to determine which network connections should be authorized for a new application, but you do not want to disable Network Security.

Subnet Masks

Many large network environments are divided into subnets to reflect an internal logic, to lower network traffic and to enhance security. For example, if you have a group of Application servers in your network that are managed by a 3rd party, that group often exists in a separate subnet.

With Network Security, you can use subnet masks to block or authorize connections specifically to a subnet. A subnet is defined through a combination of a network (IP) address (for example 172.16.0.0) with a subnet mask (for example 255.255.255.248).

Examples

- **Whitelisting**

In an environment where Network Security is enabled and uses Whitelisting, RES Workspace Manager does not allow any connections by default. The connections that users need in order to do their job must be specifically authorized.

For example, it is not enough to give the administrators of a company's Linux servers an SSH client in their RES Workspace Manager sessions. In order for the administrators to do their work, the SSH client must be authorized to connect to the Linux servers using TCP/IP over a given port. This can be achieved by creating application-level Authorized Connections for the SSH client, authorizing incoming and outgoing TCP/IP communication over port 22 to the relevant hosts.

Additional restrictions can be added as required. For example:

- Workspace Control on the authorized connection can restrict the authorized connection to a specific set of workstations. The authorized connection will only be available from computers in that Workspace, but not from other computers.
- You can create a separate authorized connection for each Linux server, and restrict each authorized connection to a set of specific administrators, so that, for example, only administrators who work in the London office can access the servers for the London office, while only the French administrators can access the servers for the French office.
- Instead of application-based Authorized Connections, you can create global ones with the relevant Access and Workspace Control.

Note

With Whitelisting, the list of blocked connections is ignored.

- **Blacklisting**

In an environment where Network Security is enabled and uses Blacklisting, RES Workspace Manager allows all connections by default. The connections that could be harmful need to be blocked for all users. Furthermore, connections that should be available *but only to specific users* need to be blocked for everybody, after which specific users should be excepted using an Authorized Connection.

For example:

- Nobody should be able to transfer information over ports 21 and 22, because these ports are often used for transferring information using FTP.
- Connection to the SQL server holding financial data should be blocked for everyone except staff of the Finance department, provided they are logging on from a computer located in the office, not from home.
- Connection to the Linux servers is blocked for everyone, but authorized for the administrators who manage those servers.

This setup can be achieved with:

- Blocked Connections that apply to all users for:
  - the database server holding the financial data
  - the Linux servers
- Authorized Connections configured for:
  - connection to database server holding the financial data with Access Control set to the members of the Finance department and Workspace Control set to the office computers.
  - connection to the Linux servers, with Access Control set to the administrators.
- An additional blocked connection for monitoring purposes so that the connections that are actually established are logged.

Notes

- With Blacklisting, an authorized connection is only useful if it narrows down a blocked connection. For example, there is no point in blocking all traffic over port 22 but specifically allowing TCP/IP traffic over port 23, as that was already allowed.
- With blacklisting, it is also possible to grant access to a specific connection for a specific group. To do so, create a blocked connection for the specific connection. Set Access Control for this connection to the specific group and select **Exclude members of Selected group**. Now this connection is blocked for everyone not in the designated group.

10.2 Performance

The Performance features in RES Workspace Manager help you get the optimal performance out of the available servers in your environment. This can be achieved by spreading the available memory and CPU capacity evenly across the server farm and across logons:

- **Access Balancing** (on page 225) sets a maximum number of simultaneous logons to RES Workspace Manager sessions on servers in a server farm. It is also possible to set different values for specific servers.
- **CPU Optimization** (on page 226) actively lowers the priority of processes with a sustained high CPU usage. This keeps the process running, but with a low priority so that other applications in the system are not hindered anymore. When the process returns to a more acceptable level of CPU usage, its priority is changed back to the original level.
- **Instant LogOff** (on page 227) ensures that user profiles unload correctly, and it disconnects the user when a log off is initiated, which improves the speed of the system as experienced by the user.
- **Memory Optimization** (on page 229) limits the maximum amount of physical memory used per session and sets a maximum number of running applications per session.

10.2.1 Access Balancing

Access Balancing limits the number of session logons that a server is allowed to process simultaneously. This optimizes the speed of logons and stabilizes a server's overall performance at peak logon times.

If many users log on at once, for example at the start of the working day or after a server reboot, this can impact the speed of session logons and the overall performance of the sessions already running on the server. Access Balancing serves as a throttle on session logons: logons that exceed the set limit are queued until the resources are available for them to be processed. Users whose logons are placed in queue are notified of their position in the queue. As a result, users no longer experience slow logons, at which only an hour glass is shown. Instead, they are informed about what is happening and how many users are ahead of them in the queue.

For example, you can set Access Balancing to allow a maximum of 2 simultaneous logons per server: If 10 users log on to a server more or less simultaneously, the first 2 logons proceed immediately and at a normal speed. Logons 3 to 10 are queued until a logon slot is freed.

Note

Administrator logons are not restricted by Access Balancing settings.

Logging

The Access Balancing Log shows detailed information about Access Balancing events.

The log also shows additional statistics about all the logons in your environment. This is useful as a basis for determining what limits to configure, but it can also contain valuable information for other purposes, for example, in relation to Service Level Agreements.

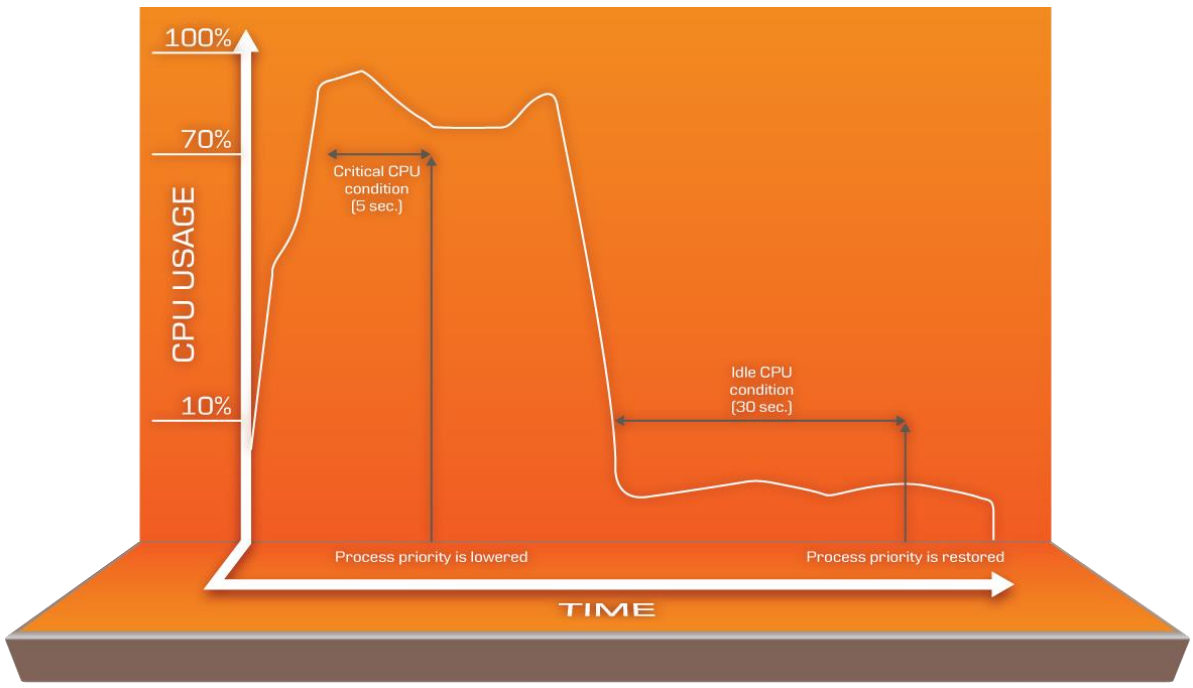
For example, the **Average queue length** specifies how many logons are held in queue on average (how many users experience a bottleneck at logon). The **Average delay** specifies how long users were held in the queue.

- If the **Average queue length** is high, while the **Average delay** is short, you can probably allow a higher number of simultaneous logons.
- If the **Average queue length** is high, while the **Average delay** is long, you may need additional server capacity.

Note

The higher the number in the field **# of logons**, the more reliable the statistics.

10.2.2 CPU Optimization



Tip

You can use **Alerting** to configure notifications for CPU Optimization events. You can find **Alerting** at **Setup > Integration > Alerting**.

Multicore machines and hyperthreading CPUs

CPU Optimization settings are independent of the number of processors: multi-CPU systems do not need other settings than single-CPU systems. If the Critical CPU condition is set to 90% on a dual-CPU system, processes will be noticed when they use 45% or more of the total CPU capacity (which is 90% of one CPU).

RES Workspace Manager regards hyperthreading and multicore CPUs as standalone CPUs. This is reflected in CPU Optimization, but also in Zones with a **Hardware Requirement** rule: 1 processor with HyperThreading / 1 dualcore processor is recognized as 2 processors in CPU Optimization and in Locations and Devices zones. As a result:

- 1 processor without HyperThreading = 1 processor in CPU Optimization / Zones
- 1 processor with HyperThreading = 2 processors in CPU Optimization / Zones
- 2 processors without HyperThreading = 2 processors in CPU Optimization / Zones
- 2 processors with HyperThreading = 4 processors in CPU Optimization / Zones
- etc.

Excluding a specific application from CPU Optimization

If a lower priority of an application affects its performance or if the application only occasionally has a high CPU utilization, you can exclude it from CPU Optimization. You can configure this by selecting the option **Exclude from CPU Optimization** on the application's **Settings** tab.

Logging

The CPU Optimization Log shows detailed information about CPU Optimization events.

The default CPU Optimization values are a critical CPU condition of 70% with an escalation period of 5 seconds, and an idle CPU condition of 10% with an probation period of 30 seconds. Use the events displayed in the CPU Optimization log to decide whether these values need to be adjusted.

If a process exceeds the configured CPU Optimization limits, you can view the measured critical CPU load duration in **Usage Tracking**, in the **Critical CPU load duration** column of the **Details** tab. This allows you to adjust CPU Optimization settings, to pinpoint "misbehaving" applications and to notice applications that need to be excluded from CPU Optimization.

10.2.3 Instant LogOff

With Instant LogOff, you can manage user profiles that fail to unload during logoff. This behavior can occur if applications do not close their registry handles when they are terminated. This behavior is usually caused by improper coding in either Microsoft software or third-party software.

- Microsoft Windows 2000 will attempt to unload the user profile 60 times at a one-second interval. After 60 seconds, during which a "Saving Settings" message will be shown to the user, the system will give up. Roaming profiles will not be reconciled.
- Microsoft Windows XP and 2003 reconcile the profile using a copy of the contents of the registry. The user does not have to wait. However, the computer cannot recover the memory used by the profile until it is unloaded. Also, users may not be able to log on again if their profile was not unloaded. This occurs, for example, if you use anonymous logons.
- In some cases (for example, when using anonymous logons), the user cannot log on if his profile cannot be unloaded.

Instant LogOff performs 2 separate actions:

- It enumerates all handles to the user registry when a user logs off, and forces them to close if they are not closed automatically. This ensures that user profiles are always unloaded. This prevents problems with the reconciliation of roaming profiles; with the registry size limit; and with the log off process to become slow (with the process remaining at "Saving Settings" for a long time).
- It disconnects users when they log off. The logoff process continues as normal after the disconnect, but users experience a faster logoff.

Note

Microsoft Windows Vista, Windows 7 and Windows Server 2008 automatically take care of user profiles that fail to unload. Instant Logoff does not need to handle this in environments where all Agents run under these operating systems. The **Disconnect** options remain relevant under those operating systems.

Instant LogOff Modes: disabled, log only, enabled

There are three Instant LogOff modes:

- In the mode **Disabled (but apply configured disconnect behavior)**, Instant LogOff does not enumerate any registry handles and does not force any to close.
- In the mode **Log only (but apply configured disconnect behavior)**, Instant LogOff log does not enumerate any registry handles and does not force any to close, but it does report any problems that occur with unloading user profiles.
- In **Enabled** mode, Instant LogOff takes action if a user profile fails to unload.

Note

The Instant LogOff mode does not affect the behavior for **Disconnect user session when log off is initiated**. If this option is selected, it is applied even if Instant LogOff is disabled or in log only mode.

Disconnect user session when logoff is initiated

In Terminal Server environments and environments that use Microsoft Windows Vista, the setting **Disconnect user session when log off is initiated** greatly enhances the speed of the system as experienced by the user. It does not affect the actual logoff process, which continues and ends normally in the disconnected session.

Enabling this feature also deactivates the "Saving Settings" message that unexpectedly pops up in Seamless Windows applications.

Notes

- If it is configured, **Disconnect user session when log off is initiated** is executed independent of the Instant LogOff mode.
- You may want to turn **Disconnect** off in test environments where users log off and then on again straight away.
- After the disconnect, the user remains logged on for a brief period of time while the logoff process continues. This is reflected, for example, in the list of User Sessions in the Management Console, where the user's name will remain visible until the session is actually logged off.

10.2.4 Memory Optimization

Memory Optimization optimizes the physical memory usage of running processes on computers in your environment. With Memory Optimization enabled, RES Workspace Manager automatically releases:

- reserved physical memory that is no longer used by a recently launched application.
- physical memory of applications that have been inactive for a while.

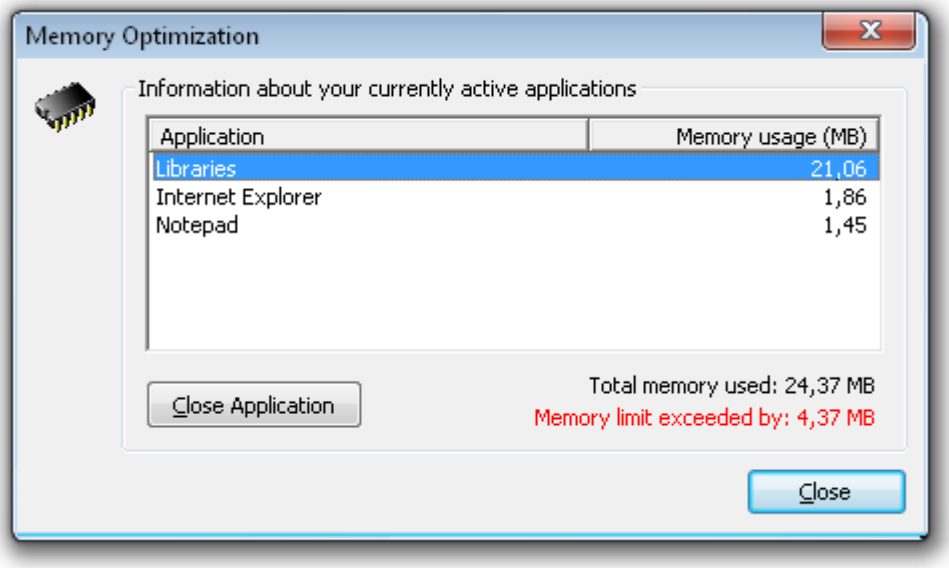
In addition, you can ensure an even spread of memory across sessions on a server by limiting:

- the amount of memory used per session.
- the number of applications that are allowed to run simultaneously in a session.

It is not recommended to use Memory Optimization alongside of other memory optimization features such as Citrix Virtual memory Optimization.

Limiting the total memory usage of a session

With the option **Limit amount of memory per session**, you can restrict the memory usage of each RES Workspace Manager session. As soon as the limit is reached, the user is not allowed to start additional applications. If a user tries to start an additional application, a message shows that memory must be freed up by closing an application. The contents of this message can be configured:



As soon as the session's memory usage drops below the configured limit, the user regains the ability to start applications.

Note

The Memory Optimization mode does not affect the options **Limit the amount of memory per session** and **Limit number of running applications per session**. If configured, these options are applied, even if Memory Optimization is disabled.

Setting Memory Optimization limits

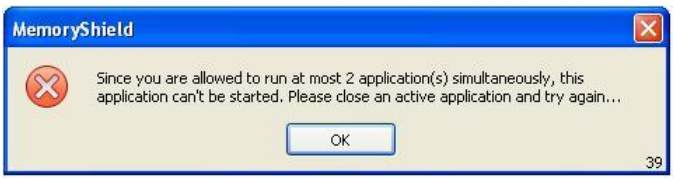
As a rule of thumb, you can use the following procedure to determine a limit for the amount of memory per session:

- Start a Terminal Server without any user sessions.
- Make a note of the amount of available memory (this is the amount of installed RAM, minus the overhead used by the OS).
- Divide the amount of available memory by the number of users who are to use this server.

The resulting number is the amount of memory that you can set per session.

Limiting the number of applications running in a session

With the option **Limit number of running applications per session**, you can restrict the number of applications that are allowed to run in any RES Workspace Manager session. Users are not allowed to start additional applications above the set limit. If a user tries to start an additional application, a message shows that an application must be closed before another one can be started. The contents of this message can be configured:



Notes

- The Memory Optimization mode does not affect the options **Limit the amount of memory per session** and **Limit number of running applications per session**. If configured, these options are applied, even if Memory Optimization is disabled.
- Memory Optimization only affects the number of running applications; not the number of open windows associated with the application.

Excluding a specific application from Memory Optimization

You can exclude an application from Memory Optimization actions:

- With the application option **Exclude from Memory Optimization Limits**, Memory Optimization will never prevent users from opening this application, even if the set Memory Optimization limits have been exceeded.
- With the application option **Exclude from Memory Optimization**, Memory Optimization will never release physical memory reserved by this application, even if it is idle. This may be necessary if the application needs its memory for background processes, for example.

Logging

If a session exceeds the Memory Optimization memory limit, this is recorded in the Memory Optimization Log. This log also records whether Memory Optimization has taken place.

- Optimizations are recorded per session after the user has logged off.
- Limits are recorded per event.

The amount of memory freed up as a result of the Memory optimizations is shown in the **Action** column of the Memory Optimization Log. This amount is cumulative for the session. For example, if Memory Optimization frees up 5 MB for a specific application, and then frees up another 5 MB at a later stage, only 5 MB of physical memory is freed up at a time, but a total amount of freed up memory is 10 MB, and this total amount is shown in the log.

Chapter 11: Management

In this chapter we will deal with managing your RES Workspace Manager environment.

11.1 Building Blocks

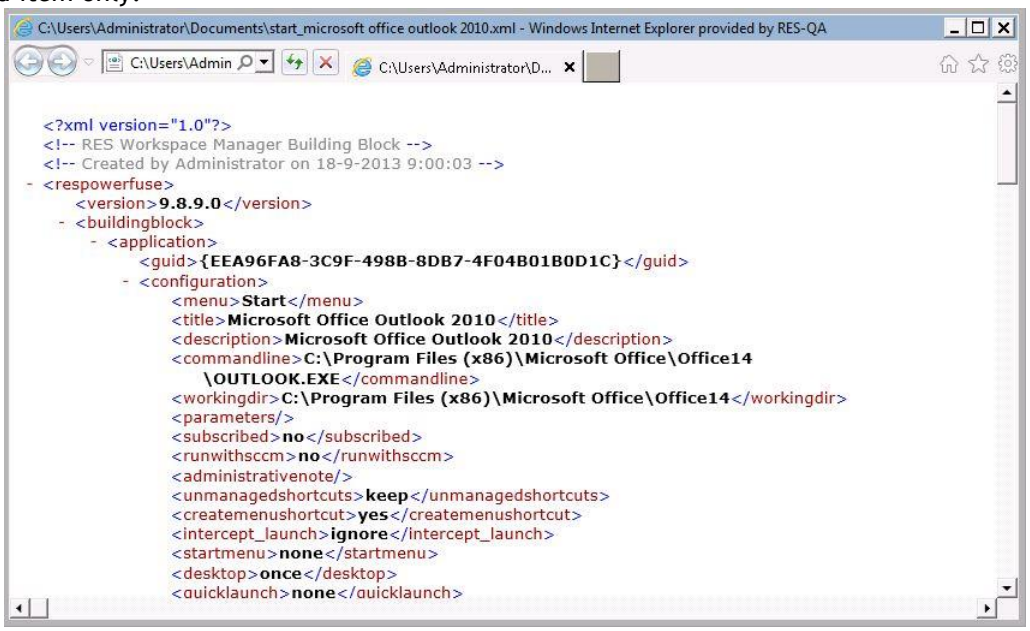
Building Blocks allow you to transport configuration settings from one RES Workspace Manager environment to another in an easy way. A Building Block is an `.xml` file that contains all properties of a certain setting or feature. This is useful as a change configuration and change management solution in e.g. DTAP environments, but also as a backup solution to facilitate disaster recovery, because Building Blocks allow you to recreate the exact configuration settings of your RES Workspace Manager environment.

With Building Blocks you can

- Use, reuse and edit an entire RES Workspace Manager environment or specific parts of it.
- Back up the configuration of an entire RES Workspace Manager environment: paper backups become obsolete with Building Blocks.
- Manage Change Management policies.
- Create predefined Building Blocks, based on best practices.
- Use an external XML-editor to edit or create Building Blocks manually.

Creating Building Blocks

To create a Building Block of a specific setting or feature, click the Building Block button next to the Instant Report button or right-click the window and select **Create Building Block**. A file save dialog will be displayed, where you can specify the name and location for the Building Block file. To create a Building Block of all settings of Zones, Actions, Data Sources, E-Mail Templates, or Security Management, right-click the item in the left tree and select **Create Building Block**. Right-click one of the items on the right side and select **Create Building Block** to create a Building Block of the selected item only.



Create Building Blocks of multiple RES Workspace Manager items at once

It is also possible to create Building Blocks of several RES Workspace Manager items at once. Select the menu option **Select items for Building Blocks** in the **Action** menu or right-click the tree on the left side of the main screen and select the option **Select items for Building Blocks**. This will expand the tree on the left with check boxes, as well as the list of applications. Each selected item will be included in the Building Blocks. Clear any application that should not be included. To create Building Blocks of selected items in the tree, right-click the main window and select **Create Building Blocks of selected items**. A dialog box will prompt you to choose between creating a single Building Block file with all selected items and creating separate Building Blocks for each item.

Importing Building Blocks

To add or update settings with a Building Block, click the Building Block button next to the Instant Report button or on the item window and select **Import Building Block** or right-click the item window, and select **Import Building Block**. A file open dialog will be displayed in which you can select the Building Block file you want to import. When importing Action settings or Security Management settings, you will be asked whether the settings from the Building Block should **replace** or **merge** with the current settings. Click **Apply** to save the new settings.

Import multiple Building Blocks at once

To import several Building Blocks at once, use the **Import Building Blocks** menu item in the **Action** menu. A dialog box will prompt you to select one or more Building Block files to import. After one or more files are selected, a dialog box will display a list of all available Building Block items in all specified files. The items in the list can be selected and cleared individually to specify which items should be imported. When the list of items contains Actions, or Security Management settings, an option will be available to specify whether the settings to import should **replace** or **merge** with the current settings. Building Blocks can only be imported for settings for which the logged on user has Write access in the Console. Click **Start import** to start processing the selected Building Blocks.

Notes

- If you import a Building Block, you can select to import the Building Block into a specific **Workspace Container**. This means that if the Building Block contains items that can be limited to a Workspace Container, these will be limited to the selected Workspace Container. Other settings associated with the items to be imported, such as Home Directory Maintenance resources, Zones, Data Sources and E-Mail templates, will also be imported. Other (global) settings and objects will not be imported from the Building Block. This is useful when consolidating configurations from several other databases and/or environments.
- When importing a Building Block, it is possible to choose whether to import Access Control settings using either **Account names** or **Account SIDs**. Based on this choice, the import process will automatically either resolve SIDs based on configured account names or resolve account names based on configured SIDs. The default setting is Account names. Unattended Building Block import will always use Account names.

Command line parameters to perform actions with Building Blocks

It is also possible to add or update settings by launching the Console with certain command line parameters.

- To import a single Building Block: `pwrtech.exe /add <path + name XML-file>`

Example: `C:\Progra~1\Ressof~1\Worksp~1\pwrtech.exe /add h:\xml\appguard_authorizedfiles.xml`

- To import several Building Blocks: `pwrtech.exe /add <path + wildcards>`

Example: `C:\Progra~1\Ressof~1\Worksp~1\pwrtech.exe /add h:\xml\*.xml`

- To delete a certain application: `pwrtech.exe /del <path + XML-file>`

Example: `C:\Progra~1\Ressof~1\Worksp~1\pwrtech.exe /del h:\xml\startmenu_accessories_calculator.xml`

To delete an application with a Building Block file, the application must first have been imported into the target database using the same GUID (that is, originating from the same source database).

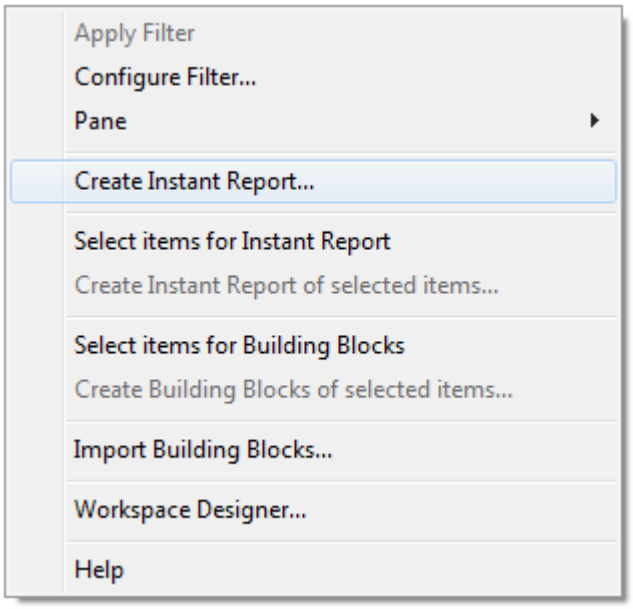
When importing Action settings or Security Management settings, add the /overwrite option to specify that these settings should replace any existing settings (for Actions, only settings for the same type (that is, "Mapping") and level (that is, "Global") will be replaced). If you do not specify this option, all settings in the specified Building Block files will be merged with the current settings.

11.2 Instant Reports

It is of the utmost importance to **document and record** all settings in the Console properly. This enables an easy-to-maintain and hand-over environment that is fully transparent, even to personnel not involved in the initial process of setting up the environment.

Instant Reports provide you with a very powerful solution to create documentation of the entire RES Workspace Manager environment. Making manual notes becomes unnecessary. Instant Reports allows you to create complete configuration, license metering and usage reports of your RES Workspace Manager environment, to gain a complete overview of used resources and their costs. Instant Reports include information about the properties and values of the documented item(s) and can include additional information about the RES Workspace Manager version.

To document your entire RES Workspace Manager environment, right-click the top node in the tree on the main window of the Console and select **Create Instant Report**.



Alternatively, you can make a selection of items to be included in the Instant Report, by selecting **Select items for Instant Report**. This will expand the tree with check boxes. Select the items that should be included in the Instant Report. Optionally, select the following items from the **Instant Report Settings** node:

- A cover page with a customizable title.
- A Table of Contents.
- "About RES Workspace Manager"
- Empty reports with non-configured settings.

Finally, select **Create Instant Report for selected items**.

To document a single feature you can also use the **Create Instant Report** button which is available at all objects that can be documented or right-click an item and select **Create Instant Report**.

You can save the generated Instant Report as a `.pdf` file, including a Table of Contents or send it to a printer directly.

11.3 Workspace Containers

Workspace Containers are logical containers that group applications and settings. With Workspace Containers, you can group applications and configuration, security and other settings in logical containers. Workspace Containers allow you to organize your environment in ways that reduce its complexity and simplify its management. You can organize your environment in many ways.

Contrary to Zones, Workspace Containers are **Agent-based**, and membership is not restricted by anything other than the logic of your own environment. It is not limited by network structure or directory services, so you can allocate Agents from different OUs to the same Workspace Container, or allocate an Agent to several Workspace Containers. This allows you to organize a complex environment in numerous ways for numerous purposes. All serving to simplify its management. For example, Workspace Containers allow you to organize your environment by:

- Computer type (e.g. laptops, desktops, Terminal Servers)
- Platform (e.g. Windows XP, Windows Vista, Windows Server 2003, Windows 7)
- Geography (e.g. countries and sites)
- Responsibility (e.g. corporate administrators and local administrators)
- Functionality (e.g. basic and advanced desktop environments or corporate and local applications)
- Customer (e.g. hosting multiple environments on shared infrastructure)
- Importance (e.g. pilot and production environments)

Example: RESDEMO

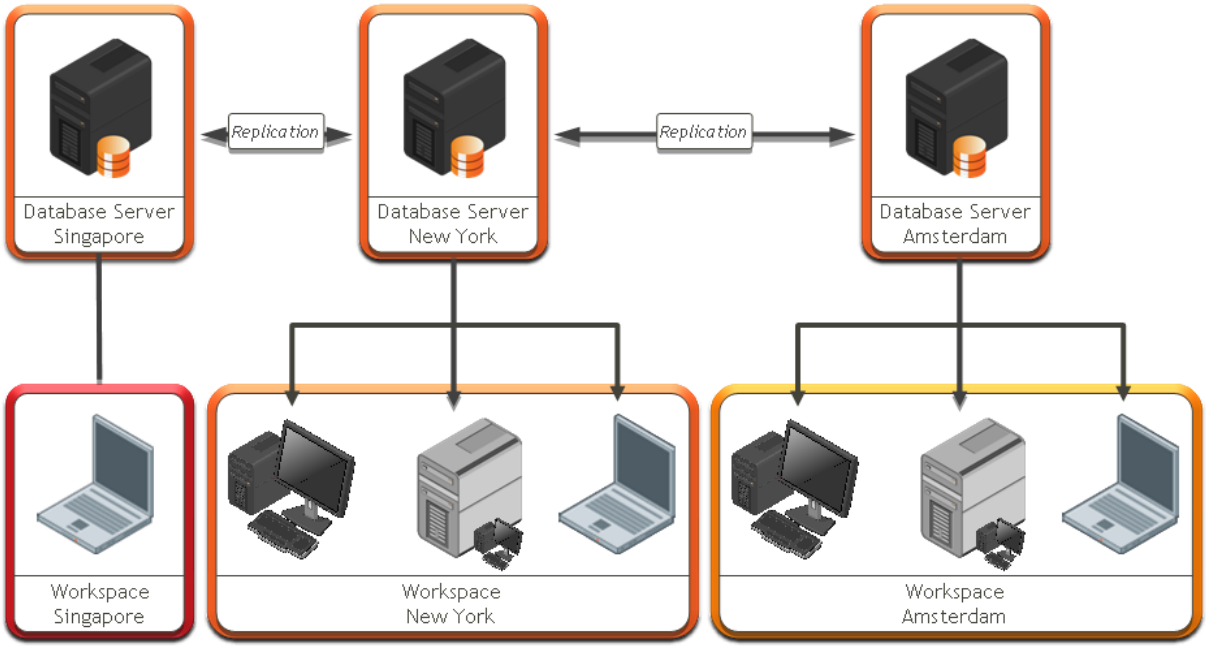
We can illustrate the concept of Workspace Containers with an example based on the fictional company RESDEMO.

RESDEMO has its headquarters in New York, where 400 people are employed. It has a sub department in Amsterdam with 200 workplaces, as well as a satellite Sales office in Singapore consisting of 20 laptops.

- The office in New York uses a mixed environment of terminal servers, workstations and laptops for 400 Agents.
- The office in Amsterdam uses a mixed environment of terminal servers, workstations and laptops for 200 Agents.
- The office in Singapore only uses laptops for 20 RES Workspace Manager Agents.

Organizing Computers in Workspace Containers

The IT manager of RESDEMO wants to organize his Agents in groups, to simplify the management of these computers. By creating three Workspace Containers - one for New York, one for Amsterdam and one for Singapore - the IT manager of RESDEMO can divide his environment in logical groups of computers and manage each group separately, as if it were a separate environment



Access Control and Workspace Containers

Many applications, configuration settings and other objects can be secured with **Access Control** and **Workspace Control**. This allows you to configure applications whose availability depends on the Workspace Container that applies to the user.

You can attach a configuration setting that is restricted to a specific Workspace Container to an application that is accessible to all Workspace Containers. This allows you to configure applications that behave differently, depending on the Workspace Container that applies to the user. See Example A.

To add an additional layer of security to your environment you can secure your Workspace Containers with access control. Access control criteria for Workspace Containers can be based on groups, users, Administrative Roles, languages and Zones. See Example B. Please note that a user can be denied access when logging on to a computer if the following conditions apply:

1. The computer is assigned to one or more Workspace Containers.
2. All assigned Workspace Containers contain Access Control.
3. The user has not been granted access to any of these Workspace Containers.

If this user does need access, a new Workspace Container needs to be added. No special configurations are necessary and this Workspace Container does not need to be added as an exception anywhere in the Management Console. The presence of this Workspace Container will give access to the users that will be denied access based on the configurations of the other Workspace Containers. The global settings will be applied for the users that fall under this Workspace Container.

Example A

Sales personnel in Singapore use the financial application Exact Finance in their daily work. The IT manager of RESDEMO has secured this application with Workspace Control criteria that are based on the Workspace Container "Singapore". This means that the application is only available for users with access to the Workspace Container "Singapore".

Example B

The IT manager of RESDEMO has secured the three existing Workspace Containers with access control:

- Workspace Container "New York" is limited by access control criteria to the OU "\\resdemo.com\New York".
- Workspace Container "Amsterdam" is limited by access control criteria to the OU "\\resdemo.com\Amsterdam".
- Workspace Container "Singapore" is limited by access control criteria to the OU "\\resdemo.com\Singapore" AND the Zone "USB stick".

The application Microsoft Outlook is used by all employees of RESDEMO. The IT manager of RESDEMO has configured this application so that it can be accessed by all RES Workspace Manager Agents and contains three E-mail settings:

- E-mail setting "Outlook for New York", which is limited by workspace control criteria to the Workspace Container "New York".
- E-mail setting "Outlook for Amsterdam", which is limited by workspace control criteria to the Workspace Container "Amsterdam".
- E-mail setting "Outlook for Singapore", which is limited by workspace control criteria to the Workspace Container "Singapore".

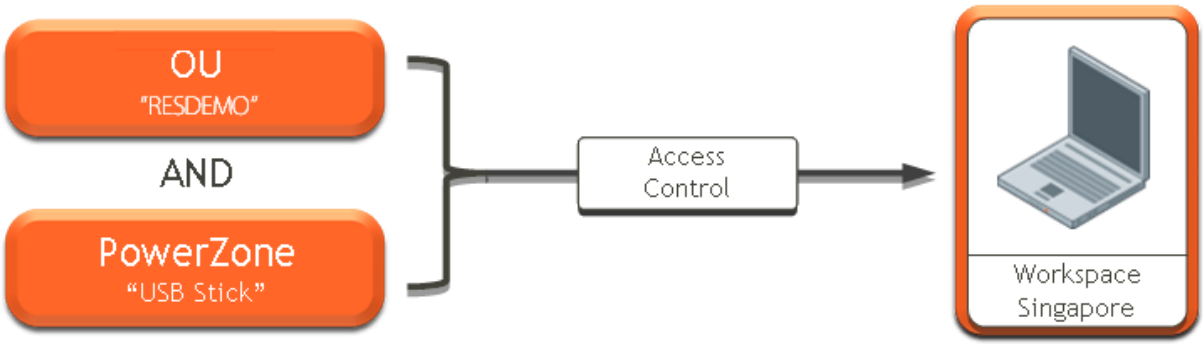
This means that when a user who belongs to the OU "\\resdemo.com\New York" logs on to an Agent in the Workspace Container "New York", only the E-mail setting that belongs to the Workspace Container "New York" will be applied. This E-mail setting has different settings than e.g. the E-mail setting for Workspace Container "Amsterdam". In this way, the IT-manager of RESDEMO has to configure one single Outlook application that behaves differently depending on the Workspace Container that applies to the user.

Example C

Because you can also assign workspace control criteria to objects in the Datastore, you can create isolated "sub-environments", which can only be accessed if their access control criteria are met.

In the RESDEMO environment, the Workspace Container "New York" should only be accessible to users that are located in New York; the Workspace Container "Amsterdam" should only be accessible to users that are located in Amsterdam and so on. You can achieve this by securing these Workspace Containers with Access Control criteria that are based on Organizational Units. This ensures that a user in e.g. Amsterdam only has access to the Workspace Container "Amsterdam" and the objects it contains if he meets the Access Control criteria of the Workspace Container. Because these Access Control criteria are based on Organizational Units, this user will not have access to the Workspace Containers "New York" and "Singapore" or any objects they contain.

The laptops in the Workspace Container "Singapore" are mainly used by sales personnel and therefore contain highly confidential information. This is why you want to secure the Workspace Container "Singapore" with additional Access Control criteria. For this purpose, the IT manager has added the Zone "USB stick" to the Access Control criteria of the Workspace Container. This Zone is based on a specific USB storage device serial number rule and ensures that users can only log on to a laptop in the Workspace Container "Singapore" if a USB stick with the correct serial number has been plugged into the laptop.



Using Workspace Containers to configure exceptions to the global settings of a feature

By default, the global settings of a feature in RES Workspace Manager apply to the entire environment. However, in certain situations you may want parts of the environment to get different settings. You can realize this by configuring exceptions for Workspace Containers. You can configure different settings for each Workspace Container in your environment.

For example, you may wish to enable the **Sessions** feature in your environment in general, but disable it for test machines. To do so, first enable and configure the **Sessions** feature as required for the environment in general. Then, add an exception for the Workspace Container "Test Machines". On this exception, you disable the **Sessions** feature. As a result, the **Sessions** feature will be disabled for all sessions to which the Workspace Container "Test Machines" apply. Sessions started outside of this Workspace Container get the global settings as configured in the **Sessions** node.

Order of priority of Workspace Containers

If you configure an exception for a Workspace Container, an extra tab will be added with the name of the Workspace Container. If you configure exceptions for several Workspace Containers, the order of the Workspace Container tabs determines the priority of the settings:

- If a user session does not fall into any of the Workspace Containers for which exceptions are configured, it gets the global settings of a feature.
- If one or more of the set Workspace Containers apply in a user's session, it gets the settings specified for the Workspace Container that has the highest priority.

Configuration

- To create an exception for a Workspace Container, click **[+]**. If the Workspace Container does not exist yet, you can create it at this point by clicking **Add**. After selecting a Workspace Container, an extra tab will be added with the name of the Workspace Container.
- To change the priority of the exceptions, right-click a Workspace Container tab and select **Increase priority** or **Decrease priority**.
- To disable or delete an exception, right-click a Workspace Container tab and select **Disable this tab** or **Delete**.

Users can choose Workspace Containers

It is possible to let users decide which accessible Workspace Container to use when starting a RES Workspace Manager session or a specific application. Effectively, this allows the user to choose between pre-defined, differently configured versions of an application or of a RES Workspace Manager session.

Choosing a Workspace Container when starting an application

- Specific Workspace Containers can be configured as a prerequisite for an application (in the application's tab **Access Control > Workspace Control**).
- RES Workspace Manager can set specific configurations for an application, for example through specific User Registry settings, and these configurations can be restricted to specific Workspace Containers.

Combined with the option to let a user choose a Workspace Container to apply to an application, users can now effectively choose the configuration with which an application should open, and they can switch between predefined application configurations.

For example, an application may be able to connect to different databases, such as database "Amsterdam" and database "Brussels". Information about the currently configured connection is stored in the Registry. When a user wants to connect the application to a different database, the information in the Registry needs to change. However, you may not want to provide the user with the database credentials and other related information.

You can set the application up with multiple database connections that are determined using User Registry actions that depend on Workspace Containers. You can let the user choose the Workspace Container when the application starts. To set this up, you need:

- Workspace Containers "Amsterdam" and "Brussels", with the same set of computers as members.
- Application X with access set to the Workspace Containers "Amsterdam" and "Brussels" (on the Workspace Control tab in Access Control), and the option Let user decide which accessible workspace container to use.
- A User Registry setting for the information that application X needs to connect to the "Amsterdam" database, with Workspace Control set to Workspace Container "Amsterdam".
- Another User Registry setting for the information that application X needs to connect to the "Brussels" database, with Workspace Control set to Workspace Container "Brussels".

Now, when the application is started, the user is asked to choose "Amsterdam" or "Brussels". Depending on this choice, RES Workspace Manager sets the Registry key to point to the chosen database.

Choosing a Workspace Container when starting a RES Workspace Manager session

Workspace Containers can also determine the configuration of an entire RES Workspace Manager session when the session starts.

To allow the user to choose in which Workspace Container the session should start, use the command line:

```
pfwsmgr.exe /ew ?
```


11.4 Workspace Analysis

The **Workspace Analysis** node is a general source of information regarding your users and can be used to gather information about the settings that have been applied to your users during logon.

Search

- The search is always restricted to a specific Directory Service.
- For a full list of all users (in a particular Directory Service), start a search without a filter or search term.
- Select a Filter to find specific kinds of users, for example users who are application manager, who have Administrative Roles, who are locked out, etc.

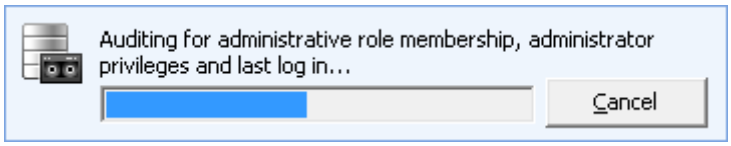
The users that are displayed at the **Workspace Analysis** node can have the following statuses:

Normal: No immediate attention required.

Dimmed: This user account is unavailable. This could indicate a password lockout or that the user account has been disabled.

Flagged: There is something special about this account. This user has unusual rights like technical manager, or a password that never expires. You can configure the triggers for the attention flag on the **Settings** tab.

Some columns are not filled out immediately, as this would cause a considerable delay before the list was complete. Right-click anywhere in the results list and choose **Audit** to fill all the empty columns. To copy information to the clipboard, right-click anywhere in the list and choose **Copy info**.



Besides the basic information that is displayed in the overview, you can gather detailed information regarding a specific user i.e. **Workspace Analysis Details** by double-clicking this user or by clicking **Analyze** in the lower right-hand corner.

Settings tab

On the **Settings** tab of the **Workspace Analysis** node, you can configure the conditions that will trigger an attention flag and specify how long event logs should be stored.

By default, each user-specific Workspace Analysis shows event logs for 3 consecutive sessions. To change this number, change the value for **Number of event logs to keep**. Note that event logs are only cleaned up once per 24 hours, indifferent of the number of event logs to keep. For example, if you have specified that event logs for 3 consecutive sessions should be kept, and the user logs on 4 times within 24 hours, 4 event logs will be kept.

Workspace Analysis - Details

Double-clicking a user will open the **Workspace Analysis Details** of the selected user. The **Workspace Analysis Details** window contains detailed information regarding the user's settings. It is more or less grouped in the same manner as the main window of the Console:

User Context

- **Locations and Devices**: The accessible Zones are based on the client and server that were used when the user last logged on to a RES Workspace Manager session.
- **Account properties**: All properties of the selected user's account. This contains all information that is available in the "basic" Workspace Analysis plus account expiration date, e-mail address, last successful authentication, LDAP user entry, assigned Administrative Roles, (in)direct membership, OU information.
- **Workspace Containers**: The Workspace Containers that are currently active for this user.

Composition

The **Applications** section contains the following information:

- **Applications**: All applications that the user has access to, plus who authorized access to the application (if applicable).
    - **File Types**: The File Types configured for this user. That is, for which available applications file associations have been configured.
    - **E-mail Settings**: E-mail Settings that are attached to applications to which the user has access. E-mail Settings that are not attached to an application, but that do belong to the scope of the user, will not be displayed.
    - **Data Sources**: The Data Sources that are attached to applications to which the user has access. Data Sources that are not attached to an application, but that do belong to the scope of the user, will not be displayed.

The **Actions By Event** section contains information on all of the user's Actions, grouped by the session event that triggers them and listed in the order of execution:

- **At logon**: May contain actions for Environment Variables, Folder Redirection, Automation Tasks, Microsoft ConfigMgr, Execute Command, Drive and Port Mappings, Drive Substitutes, Printers, User Home Directory, Folder Synchronization, User Registry and User Profile Directory
- **At Session Refresh**: May contain actions for Folder Synchronization and Execute Command.
- **At Session Reconnect**: May contain actions for Folder Synchronization and Execute Command.
- **At Logoff**: May contain actions for Folder Synchronization and Execute Command.

The **Actions By Type** section contains the following information:

- **RES Automation Manager Tasks**: An overview concerning the user's RES Automation Manager Tasks.
- **Environment Variables**: An overview of the user's Environment Variable Actions.
- **Execute Command**: An overview of the user's Execute Command Actions.

The **Files and Folders** section contains the following information:

- **Drive and Port mappings**: An overview of the user's Mappings. The last logon is used to determine which language should be used when showing language-based settings.
- **Drive Substitutes**: An overview of the user's Drive Substitutes.
- **Folder Redirection**: An overview of the user's Folder Redirections.
- **Folder Synchronization**: An overview of the user's Folder Synchronizations.
- **User Home Directory**: An overview of the user's Home Directory Actions.
- **User Profile Directory**: An overview of the user's Profile Directory Actions.

- **LANDesk**: An overview concerning the user's LANDesk software distributions.
- **Microsoft ConfigMgr**: An overview concerning the user's Microsoft ConfigMgr Distributions.
- **Printers**: All configured Network Printers for the user.
- **User Registry**: An overview of the user's Registry Settings. When viewing the user's registry settings, double-clicking **End result** (at the bottom of the **Type** column) will merge all configured registry settings and show the end result in the Registry Viewer. To track registry values, the source is shown on the right.
- **User Settings**: All configured User Settings for the user.

 **Security** (only applicable to the Gold license edition of RES Workspace Manager)

The **Applications** section contains the following information:

- **Managed Applications**: The Applications log for the specific user provides an overview of the applications that were blocked for this user.
- **User Installed Applications**: All User Installed Applications (if applicable).
- **Websites**: The websites log for the specific user provides an overview of all blocked attempts to access websites for this user.

The **Data** section contains the following information:

- **Removable Disks**: The Removable Disks Access for the specific user provides an overview about the user's access to removable media. The log provides an overview of all blocked attempts to access a removable disk for this user.
- **Files and Folders**: The Files and Folders log for the specific user provides an overview of the files and folders that were blocked for this user.
- **Read-Only Blanketing**: The Read-Only Blanketing log for the specific user provides an overview of all blocked attempts to access a drive that is rendered read-only for this user.
- **Network connections**: The Network Connections log for this user provides an overview of all blocked network connections for this user.
- **User Sessions**: The User Sessions log provides a detailed list of all Sessions security events for this user.

Diagnostics

- **User sessions**: A list of the user's active sessions. Right-click a session in this list to force a refresh of the session, remote control the session, etc.
- **Workspace Model Overview**: An overview of the mode in which each RES Workspace Manager feature is running, including information about any Workspace Container exception that applies to the user.
- **Event Log**: A Log of all **Action** settings that were processed for this user. Use the event log option to find problems with a user's settings.
- **Usage Tracking**: Double-click the **Details** pane to open the Usage Tracking viewer for the selected user.
- **Delegated access control**: The applications of which the user is an application manager. Selecting an application displays all details of the delegated application (users, capacity in use, etc.).

The **Performance** section contains the following information:

- **Access Balancing**: The Access Balancing log provides a detailed list of all Access Balancing events for this user.
- **CPU Optimization**: The CPU Optimization log provides a detailed list of all CPU Optimization events for this user.
- **Instant LogOff**: The Instant LogOff log provides a detailed list of all Instant LogOff events for this user.
- **Memory Optimization**: The Memory Optimization log provides a detailed list of all Memory Optimization events for this user.

Tip

The **Workspace Analysis Details** window can be minimized to the Taskbar, which allows you to browse the Console while still having quick access to the Workspace Analysis overview for the selected user.

11.5 Errors

Use the **Errors** node of the **Diagnostics** section to display information about the errors that occurred in your RES Workspace Manager environment.

- Use the check box to filter the entries in the log.
- To view the properties of an event, right-click it and click **Properties** in the context menu.
- To clear the log, right-click an event and click **Clear** in the context menu.

Chapter 12: Contact Information

Headquarters	
RES Software International Het Zuiderkruis 33 5215 MV 's-Hertogenbosch The Netherlands Phone: +31 (0)73 622 8800 Fax: +31 (0)73 622 8811	**RES Software USA** Radnor Financial Center 150 North Radnor Chester Road Suite D100 Radnor, PA 19087 USA Phone: +1 800-893-7810
E-mail: info@ressoftware.com Portal: http://support.ressoftware.com Community: http://www.resug.com Website: http://www.ressoftware.com Twitter: @ressoftware	
Regional Offices	
For the addresses of our regional offices, see http://www.ressoftware.com	
RES Marketing	
RES Marketing:	marketing@ressoftware.com
RES Back Office	
To order licenses, course materials etc:	backoffice@ressoftware.com

Chapter 13: Index

A

Access Balancing • 225
Access Control • 52, 81, 102
Actions • 112
Additional User Setting options • 155
Administrative Roles • 67
Agent Prerequisites • 220
Agents • 36
Alerting • 161, 184
Allow users to restore their own settings • 157
Application Delegation • 65
Application level • 206, 221
Application Management • 87
Application Virtualization • 163
Applications • 87, 88, 205
Applications security modes
  disabled, learning, enabled • 205
Applications User Settings • 158
Architecture • 8
Assigning permissions to users • 215
Audit Trail • 203
Authorized Connections • 208
Authorized Files • 204, 206, 218
Authorizing a specific application to use specific connections • 222
Authorizing files and folders • 218
Automation Tasks • 133

B

Background • 138
Blacklisting • 223
Building Blocks • 196, 231

C

Central storage location of User Settings and other user-specific information • 153, 154
Citrix streamed applications • 160
Citrix XenApp Publishing • 163
Citrix XenApp Streaming • 163, 170
Communication Model • 13
Components • 8
Composition • 74
Configuration • 104
Configuration Wizard • 26
Configuring Applications • 93
Configuring Automation Tasks • 133
Configuring commands • 130
Configuring different settings for certain parts of the environment • 219
Configuring Drive and Port Mappings • 113
Configuring Drive Substitutes • 115
Configuring Environment Variables • 135
Configuring folder redirection • 118
Configuring folder synchronization • 120
Configuring linked actions • 136
Configuring printers • 123
Configuring registry policies • 129
Configuring Registry Settings • 125
Configuring the Shell - Centralized Computing • 20, 22
Configuring User Installed Applications • 210
Configuring Website Security • 212
Configuring Workspace Extensions • 110
Connection States • 63
Contact Information • 245
CPU Optimization • 225, 226
Create a drive mapping using information from Active Directory • 114
Creating a Blocked Connection for monitoring purposes in Blacklisting environments • 222

D

Data • 214
Data Sources • 106, 109
Default behavior if running applications are no longer authorized • 206
Default Hide drives behavior • 114
Defaults for new applications • 92
Desktop • 137
Desktop Sampler • 83
Desktop Transformation • 82
Directory Maintenance • 121
Directory Services • 47
Disconnect user session when logoff is initiated • 228
Drive and Port Mappings • 112
Drive mappings • 215
Drive Substitutes • 115
Dynamic Privileges • 209

E

E-mail Settings • 105, 108
Environment Variables • 135
Errors • 244
Example • 135
  blocking and authorizing files • 216
  Using a USB device for authentication purposes • 62
Examples • 118, 213, 223
Exceptions to blocked connections when Blacklisting • 222
Excluding a specific application from CPU Optimization • 227

Excluding a specific application from Memory Optimization • 230
Excluding certain types of users • 219
Excluding passthrough sessions • 220
Execute Command • 130
Exempting an application from Network Security Settings • 222

F

File Types • 107
Files and Folders security • 205, 216
Files and Folders security Mode
disabled, learning, enabled • 216
Filters • 71
Folder Redirection • 116
Folder Synchronization • 119

G

Generic Isolation Integration • 163, 170, 176
Global level • 205, 221
Global Network Security and application-based Authorized Connections • 222

I

Identity • 52
Individual blocked connections • 221
Installation & Setup • 16
Installing RES Workspace Manager and Configuring the Shell • 19
Installing the Desktop Sampler • 83
Instant LogOff • 225, 227
Instant LogOff Modes
disabled, log only, enabled • 228
Instant Passthrough for Citrix XenApp • 166, 168
Instant Passthrough for Microsoft TS RemoteApp • 174, 175
Instant Reports • 196, 234
Integrating File Types with Workspace Extensions • 111
Integration • 161
Introduction • 1
Introduction to Desktop Transformation • 82
Introduction to User Workspace Management • 5

L

LANDesk • 132, 182
Language Identity • 129
Languages • 64
License metering • 201
Licensing • 99, 207
Licensing Model • 39
Licensing Process • 41
Limiting the number of applications running in a session • 230
Limiting the total memory usage of a session • 229
Linked Actions • 136
Linking • 156
Locations and Devices
Zones • 56
Lockdown and Behavior • 79, 139
Logging • 209, 215, 217, 218, 220, 226, 227, 230

M

Managed Applications • 86, 205
Security section • 206
Management • 231
Managing Licenses • 39, 43
Memory Optimization • 225, 229
Microsoft App-V • 163, 171
Microsoft App-V applications • 160
Microsoft Remote Assistance • 180
Microsoft System Center • 181
Microsoft System Center Configuration Manager Software Distributions • 131
Microsoft TS RemoteApp • 163, 173
Migration settings when switching to another Zero Profile mode • 150
Multicore machines and hyperthreading CPUs • 227
Multiple Rules for a Zone • 60

N

Network Connections security • 220
Network Security Modes
disabled, learning, enabled • 221
Novell Directory Services • 49

O

Override local caching • 158

P

Pattern matching in Zones • 61
Performance • 225
PowerHelp • 81
Prerequisites • 17, 119
Printers • 123
Printing Preferences • 80
Process Interception for unmanaged shortcuts • 89, 91
Properties • 93

R

Read-Only Blanketing • 217
Read-Only Blanketing security Modes
disabled, learning, enabled • 217
Relay Servers • 31
Removable Disks security • 214
Removable Disks security modes
disabled, learning, enabled • 214
RES Automation Manager • 183, 184
RES HyperDrive • 183, 186
RES IT Store • 55, 183, 187
RES Software • 183
RES VDX • 183, 188

RES Workspace Manager Licensing • 39
RES Workspace Manager modules • 39, 45
RES Workspace Manager Relay Servers • 11

S

Sampling • 155
Save printing preference • 157
Scope Control • 67, 69
Screensaver • 139
Security • 204
Security & Performance • 204
Security Method
  Whitelisting or Blacklisting • 221
Setting Memory Optimization limits • 230
Setting up the Datastore • 24
Settings tab • 88
Shell • 137
Start Menu Tab • 87
Storage method • 152
Storage of users' User Setting data • 152
Subnet Masks • 222

T

The End-User Workspace • 74
The RES Workspace Composer • 12
The RES Workspace Manager Agent Cache • 15
The RES Workspace Manager Agent Service and its sub processes • 14
The RES Workspace Manager Agents • 9
The RES Workspace Manager Console • 8
The RES Workspace Manager Datastore • 9
The Workspace Composer • 75
Toggle Remove • 129
Track any changed setting within scope immediately (global) • 147
Track any setting changed by application immediately (application) • 148
Tracking and Reporting • 192

U

Usage Tracking • 192
Usage Tracking Overview • 194
User Installed Applications • 210
User Registry • 125, 145
User Sessions • 195
User Sessions security • 219
User Settings • 107, 140, 160
User Settings Caching • 153, 154
User Workspace Management • 5
Using Locations and Devices for Printers • 125

V

Variables and special folders • 147, 148, 159
Video Tutorials • 2

W

Web Portal • 191
Websites • 212
What is saved as part of a Targeted Item • 151
Whitelisting • 223
Workspace Analysis • 69, 105, 122, 196, 241
Workspace Branding • 51
Workspace Containers • 67, 235
Workspace Designer • 85
Workspace Extensions • 110
Workspace Model • 86
Workspace Preferences • 77
Workspace Simulation Wizard • 197

Z

Zero Profile Modes • 141
Zone Members
  Nested Zones • 61
Zone rules • 56